

The author(s) shown below used Federal funds provided by the U.S. Department of Justice and prepared the following final report:

Document Title: A Comprehensive Report on School Safety Technology

Author(s): Johns Hopkins University Applied Physics Laboratory

Document No.: 250274

Date Received: October 2016

Award Number: 2013-MU-CX-K111

This report has not been published by the U.S. Department of Justice. To provide better customer service, NCJRS has made this federally funded grant report available electronically.

<p>Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.</p>

A Comprehensive Report on **School Safety Technology**

Prepared for
The Department of Justice's
National Institute of Justice

NIJ | *National Institute
of Justice*

Prepared by
The Johns Hopkins University Applied Physics Laboratory
in cooperation with
The Johns Hopkins University School of Education,
Division of Public Safety Leadership



NATIONAL CRIMINAL JUSTICE TECHNOLOGY
RESEARCH, TEST & EVALUATION CENTER
POLICE • COURTS • CORRECTIONS

The research described in this report was sponsored by the National Institute of Justice, prepared and conducted by The Johns Hopkins University Applied Physics Laboratory (APL) in cooperation with The Johns Hopkins University School of Education, Division of Public Safety Leadership, and The Bloomberg School of Public Health.



Published by The Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland
© Copyright 2016 by The Johns Hopkins University Applied Physics Laboratory

For more than 70 years, APL has provided critical contributions to critical challenges with systems engineering and integration, technology research and development, and analysis. As the Nation's largest University-Affiliated Research Center, APL undertakes vital national security and scientific challenges in a way that is free from conflicts of interest or competition with commercial industry.

www.jhuapl.edu

Task No.: FGSGJ
Contract No.: 2013-MU-CX-K111/115912
Tracking No.: AOS-15-0643

This project was supported by Award No. 2013-MU-CX-K111, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.



ACKNOWLEDGMENTS

The preparation of this report required the dedication of many people. Firstly, we thank all the contributing authors for their extraordinary effort and dedication in preparing the book chapters within a very tight timeframe. Secondly, we state our gratitude to all the reviewers whose critical and constructive feedback greatly improved the quality of the report. Thirdly, we express our appreciation for the many individuals who contributed their time in ways large and small; they were instrumental in shaping our thinking about school safety and security. These people include Jeff Allison, Alan Bragg, John Buettner, Jeff Derreth, Paul Dillon, Kevin Burnett, Mo Canady, Edward Clarke, Michael Dorn, Larry Faries, Michele Gay, Drew Gerber, Jennifer Golbeck, Guy Grace, Calvin Hodnett, Dennis McClimans, Ronald Miller, Eric North, Cynthia Pappas, Sue Stein, Terry Street, Madeline Sullivan, Duane Williams, F. Michael Wyant, Michael Yorio, and John Young. We hope your thoughts and statements are accurately portrayed; any errors are the responsibility of the authors.

Lastly, we thank National Institute of Justice staff member William Ford for his support throughout the preparation of this report.

This job of keeping our children safe, and teaching them well, is something we can only do together, with the help of friends and neighbors, the help of a community, and the help of a nation.

—President Barack Obama, 16 December 2012

All children should grow up free from fear and violence.

—U.S. Department of Education

School leaders must develop proactive systems to address school safety that include all stakeholders. This includes creating a personalized, safe, orderly, and inviting school environment predicated on nurturing relationships and shared responsibility.

—National Association of Secondary School Principals

CONTENTS

	Page
ACKNOWLEDGMENTS.....	III
LIST OF ILLUSTRATIONS.....	XIII
LIST OF TABLES.....	XVII
EXECUTIVE SUMMARY	ES-1
CHAPTER 1. INTRODUCTION	1-1
1.1 Purpose	1-1
1.2 Background	1-2
1.3 Schools	1-3
1.4 Approach to the Tasks.....	1-4
1.5 Limitations.....	1-5
1.6 How to Use this Document	1-7
1.7 Study Team.....	1-9
CHAPTER 2. SCHOOL SAFETY AND SECURITY TECHNOLOGY IMPLEMENTATION PLANNING	2-1
2.1 Introduction	2-1
2.2 Background	2-2
2.3 The Planning Process.....	2-3
2.4 Planning Teams	2-5
2.5 Understand the Situation	2-6
2.5.1 Identify Assets.....	2-7
2.5.2 Identify Threats	2-8
2.5.3 Establish Likelihood.....	2-9
2.5.4 Identify Vulnerabilities.....	2-10
2.5.5 Identify Consequences.....	2-12
2.5.6 Assess Risk	2-12
2.6 Determine Goals and Objectives and Select Courses of Action	2-14
2.7 Select Technology	2-17
2.7.1 Cyberspace Security.....	2-20
2.7.2 Technology Integration	2-20
2.7.3 Safety Planning	2-21
2.8 Iterate.....	2-21
2.9 Conclusion.....	2-22
2.10 Further Reading.....	2-22
CHAPTER 3. TECHNOLOGY REVIEW – ACCESS CONTROL	3-1
3.1 Introduction	3-1
3.2 Utilization Statistics.....	3-4
3.3 Physical Barriers	3-4
3.3.1 Locks	3-4
3.3.2 Fencing.....	3-11
3.3.3 Turnstiles and Man-Traps	3-17
3.3.4 Vehicle Barriers	3-25
3.3.5 Bullet-Resistant Doors and Coverings.....	3-32
3.3.6 Bullet-Resistant Windows and Films.....	3-39
3.3.7 Lockdown Devices.....	3-46

CONTENTS (CONTINUED)

	Page
3.4 Identification Cards	3-55
3.4.1 Introduction	3-55
3.4.2 How the Technology Is Used.....	3-55
3.4.3 What Makes the Technology Good?.....	3-56
3.4.4 Concerns About the Technology.....	3-58
3.4.5 Cost Considerations	3-59
3.4.6 Emerging Technologies and Future Considerations	3-60
3.4.7 Current Vendors.....	3-60
3.5 Conclusion	3-60
CHAPTER 4. TECHNOLOGY REVIEW – ALARMS AND SENSORS.....	4-1
4.1 Introduction	4-1
4.2 Utilization Statistics	4-3
4.3 Intrusion and Access Sensors	4-4
4.3.1 Motion Sensors	4-4
4.3.2 Photoelectric Beam Sensors	4-12
4.3.3 Open-Door Sensors	4-19
4.4 Duress Alarms	4-26
4.4.1 Introduction	4-26
4.4.2 How the Technology Is Used.....	4-28
4.4.3 What Makes the Technology Good?.....	4-29
4.4.4 Concerns About the Technology.....	4-33
4.4.5 Cost Considerations	4-34
4.4.6 Emerging Technologies and Future Considerations	4-35
4.4.7 Current Vendors.....	4-35
4.5 Further Reading.....	4-35
4.6 Conclusion	4-35
CHAPTER 5. TECHNOLOGY REVIEW – COMMUNICATIONS.....	5-1
5.1 Introduction	5-1
5.2 Two-Way Communications	5-4
5.2.1 Two-Way Radios	5-4
5.2.2 Intercoms and Public Address Systems	5-12
5.2.3 Emergency Call Boxes	5-19
5.2.4 Telephone Systems	5-24
5.3 One-Way Communications	5-30
5.3.1 Emergency Notification Systems	5-30
5.3.2 Bullhorns	5-34
5.3.3 Digital Signs and Billboards	5-37
5.3.4 Datacasting	5-41
5.4 Conclusion	5-46
CHAPTER 6. TECHNOLOGY REVIEW – LIGHTING	6-1
6.1 Introduction	6-1
6.2 Utilization Statistics	6-2

CONTENTS (CONTINUED)

	Page
6.3 Indoor Security Lighting	6-3
6.3.1 Introduction	6-3
6.3.2 How the Technology Is Used.....	6-4
6.3.3 What Makes the Technology Good?.....	6-5
6.3.4 Concerns About the Technology.....	6-6
6.3.5 Cost Considerations	6-7
6.3.6 Emerging Technologies and Future Considerations	6-8
6.3.7 Current Vendors.....	6-8
6.4 Outdoor Security Lighting	6-9
6.4.1 Introduction	6-9
6.4.2 How the Technology Is Used.....	6-11
6.4.3 What Makes the Technology Good?.....	6-12
6.4.4 Concerns About the Technology.....	6-15
6.4.5 Cost Considerations	6-15
6.4.6 Emerging Technologies and Future Considerations	6-17
6.4.7 Current Vendors.....	6-17
6.5 Conclusion	6-17
CHAPTER 7. TECHNOLOGY REVIEW – SOFTWARE APPLICATIONS.....	7-1
7.1 Introduction	7-1
7.2 Utilization Statistics.....	7-4
7.3 Software Applications	7-4
7.3.1 Security Planning Tools	7-4
7.3.2 Physical Security Information Management.....	7-9
7.3.3 Violence Prediction Software.....	7-16
7.3.4 Visitor Database Checks.....	7-18
7.3.5 Mental and Public Health Information Sharing	7-24
7.3.6 Social Media Monitoring and Communication	7-25
7.3.7 Tip Lines	7-30
7.4 Conclusion	7-36
CHAPTER 8. TECHNOLOGY REVIEW – SURVEILLANCE	8-1
8.1 Introduction	8-1
8.2 Utilization Statistics.....	8-3
8.3 Surveillance Cameras	8-4
8.3.1 Introduction	8-4
8.3.2 How the technology is used.....	8-5
8.3.3 What makes the technology good?	8-6
8.3.4 Concerns about the technology.....	8-13
8.3.5 Cost Considerations	8-14
8.3.6 Emerging Technologies and Future Considerations	8-15
8.3.7 Current Vendors.....	8-15
8.4 Gunshot Location Systems	8-16
8.4.1 Introduction	8-16
8.4.2 How the Technology is Used.....	8-17
8.4.3 What Makes the Technology Good.....	8-17

CONTENTS (CONTINUED)

	Page
8.4.4 Concerns about the Technology	8-19
8.4.5 Cost Considerations	8-20
8.4.6 Emerging Technologies and Future Considerations	8-21
8.4.7 Vendors.....	8-21
8.5 Location Tracking Systems	8-22
8.5.1 Introduction	8-22
8.5.2 How is the Technology Used.....	8-22
8.5.3 What Makes the Technology Good.....	8-23
8.5.4 Concerns about the Technology	8-26
8.5.5 Cost Considerations	8-28
8.5.6 Emerging Technologies and Future Considerations	8-29
8.5.7 Vendors.....	8-29
8.6 Unmanned Aerial Vehicles	8-30
8.6.1 Introduction	8-30
8.6.2 How the Technology is Used.....	8-30
8.6.3 What Makes the Technology Good.....	8-30
8.6.4 Concerns about the technology.....	8-32
8.6.5 Cost Considerations	8-33
8.6.6 Emerging Technologies and Future Considerations	8-34
8.6.7 Current Vendors.....	8-34
8.6.8 Further Reading	8-35
8.7 Conclusions	8-35
CHAPTER 9. TECHNOLOGY REVIEW – WEAPONS DETECTION	9-1
9.1 Introduction	9-1
9.2 Utilization Statistics.....	9-2
9.3 Personnel Systems	9-3
9.3.1 Introduction	9-3
9.3.2 How the Technology Is Used.....	9-3
9.3.3 What Makes the Technology Good?.....	9-4
9.3.4 Concerns about the Technology	9-7
9.3.5 Cost Considerations	9-8
9.3.6 Emerging Technologies and Future Considerations	9-9
9.3.7 Current Vendors.....	9-9
9.4 Baggage Systems.....	9-10
9.4.1 Introduction	9-10
9.4.2 How the Technology Is Used.....	9-10
9.4.3 What Makes the Technology Good?.....	9-11
9.4.4 Concerns about the Technology	9-13
9.4.5 Cost Considerations	9-14
9.4.6 Emerging Technologies and Future Considerations	9-15
9.4.7 Current Vendors.....	9-16
9.5 Conclusion	9-16

CONTENTS (CONTINUED)

	Page
CHAPTER 10. TECHNOLOGY REVIEW – OTHER TECHNOLOGY SYSTEMS	10-1
10.1 Introduction	10-1
10.2 Utilization Statistics	10-3
10.3 Personal Protection – Bullet-Resistant Shields	10-3
10.3.1 Introduction	10-3
10.3.2 How the Technology Is Used	10-4
10.3.3 What Makes the Technology Good?	10-6
10.3.4 Concerns About the Technology	10-7
10.3.5 Cost Considerations	10-8
10.3.6 Emerging Technologies and Future Considerations	10-9
10.3.7 Current Vendors	10-10
10.3.8 Further Reading	10-10
10.4 Personal Protection – Privacy Window Film	10-11
10.4.1 Introduction	10-11
10.4.2 How the Technology Is Used	10-12
10.4.3 What Makes the Technology Good?	10-12
10.4.4 Concerns About the Technology	10-14
10.4.5 Cost Considerations	10-14
10.4.6 Emerging Technologies and Future Considerations	10-15
10.4.7 Current Vendors	10-15
10.4.8 Further Reading	10-16
10.5 Conclusion	10-17
CHAPTER 11. SCHOOL DISTRICT CASE STUDIES	11-1
11.1 Introduction	11-1
11.2 Methodology	11-2
11.2.1 Case Study Rationale	11-2
11.2.2 Strengths and Limitations	11-2
11.2.3 Approach	11-2
11.3 Case Study District One	11-5
11.3.1 District Description	11-5
11.3.2 School Safety Technologies in Use	11-7
11.3.3 Integration	11-9
11.3.4 Challenges and Concerns	11-10
11.3.5 School Safety Technology List	11-10
11.4 Case Study District Two	11-13
11.4.1 District Description	11-13
11.4.2 School Safety Technologies in Use	11-14
11.4.3 Integration	11-17
11.4.4 Challenges and Concerns	11-17
11.4.5 School Safety Technology List	11-18
11.5 Case Study District Three	11-21
11.5.1 District Description	11-21
11.5.2 School Safety Technologies in Use	11-23

CONTENTS (CONTINUED)

	Page
11.5.3 Integration	11-26
11.5.4 Challenges and Concerns	11-26
11.5.5 School Safety Technology List	11-26
11.6 Case Study District Four	11-29
11.6.1 District Description	11-29
11.6.2 School Safety Technologies in Use	11-30
11.6.3 Implementation Aspects of Technology	11-32
11.6.4 Integration	11-33
11.6.5 Challenges and Concerns	11-33
11.6.6 School Safety Technologies in Use	11-33
11.7 Conclusion	11-37
CHAPTER 12. LEGAL REVIEW	12-1
12.1 Introduction	12-1
12.2 Methodology	12-2
12.2.1 Data Collection	12-2
12.2.2 Analysis	12-3
12.2.3 Results	12-5
12.3 Discussion	12-24
12.4 Strengths and Limitations	12-26
12.5 Conclusion	12-26
CHAPTER 13. LITERATURE REVIEW	13-1
13.1 Introduction	13-1
13.1.1 Methodology	13-1
13.2 Types of Schools	13-2
13.3 Defining School Safety	13-3
13.3.1 Current Data about School Safety	13-3
13.3.2 What is a Safe School?	13-4
13.3.3 Perceptions of School Safety and Technology	13-5
13.4 School Safety Technologies	13-7
13.4.1 Types of Available Technology	13-7
13.4.2 What Technology is in Use	13-11
13.5 Safety Technology Selection and Evaluation	13-12
13.5.1 The Decision-Making Process	13-12
13.5.2 Identifying the Threat	13-13
13.5.3 Quantifying Effectiveness of Technologies	13-14
13.5.4 Resources for Decision-Makers	13-15
13.6 Findings	13-20
13.6.1 School Safety	13-21
13.6.2 Summary	13-21

CONTENTS (CONTINUED)

	Page
CHAPTER 14. INTERNATIONAL SCHOOL SAFETY TECHNOLOGY REVIEW	14-1
14.1 Introduction	14-1
14.2 Points of Focus	14-3
14.3 Background	14-4
14.4 Challenges in Developing and Underdeveloped Nations	14-5
14.5 Perspective on School Security Technology, Worldwide Approaches, and Global Conflict.....	14-5
14.5.1 Overview of School Violence and Technology in a Selection of Nations	14-6
14.5.2 Study of School-based Violence in Five Asian Nations	14-14
14.6 Conclusion	14-14
CHAPTER 15. CONCLUSION	15-1
APPENDIX A. REFERENCES	A-1
APPENDIX B. CASE STUDY QUESTIONNAIRE	B-1
APPENDIX C. ACRONYMS	C-1

This page intentionally left blank.

LIST OF ILLUSTRATIONS

	Page
2-1 Risk Assessment Process Model	2-7
2-2 School Defense-in-Depth Layers	2-11
2-3 Semi-quantitative Risk Assessment	2-13
2-4 Sample Risk Assessment Worksheet.....	2-14
2-5 Notional Technology Choices.....	2-20
3-1 Examples of Fences’	3-12
3-2 Example of Decorative Fences’	3-13
3-3 Examples of Vehicle Barriers.....	3-25
3-4 Example of a Concrete Planter Vehicle Barrier	3-28
3-5 Examples of Doors with Lights and Sidelights.....	3-33
3-6 Samples of Bullet-Resistant Panels, with Corkboard and Dry Erase Board Surfaces, Attached to Standard Doors	3-34
3-7 Example of a Bullet-Resistant Transaction Window that Allows Conversation and the Passing of Small Items Safely Underneath	3-40
3-8 Window Film Provided on Rolls	3-41
3-9 Bullet-Resistant Windows	3-42
3-10 Parts of Typical Door Lock Showing Moveable Latch Bolt and Hole in Strike Plate	3-46
3-11 Examples of Anti-Latch Devices	3-48
3-12 Example of Security Bar Installed To Form a Brace Between Door Knob and Floor, which Inhibits Opening the Door Inward	3-49
3-13 Examples of Metal Sleeve and Strap Options to Prevent a Hydraulic Door from Opening	3-49
3-14 Examples of Anti-Breach Devices that Anchor Door to Surrounding Structure.....	3-50
4-1 Sensors and Alarms Integration with School Stakeholders.....	4-1
4-2 Motion Detection Process.....	4-5
4-3 Corner-Mounted Motion Sensor Location and Detection Area.....	4-6
4-4 Detection Area for Ceiling-Mounted Motion Sensors	4-6

LIST OF ILLUSTRATIONS (CONTINUED)

	Page
4-5	Photoelectric Beam Detector Types4-14
4-6	Photoelectric Beam Process.....4-14
4-7	Photoelectric Beam Installation Used Outdoors and Indoors.....4-15
4-8	Door Open Sensors for Magnetic and Contact4-19
4-9	Open-Door Process4-20
4-10	Open-Door Sensors Mounted to Door.....4-21
4-11	Process for Human-Triggered Alarms4-28
5-1	Examples of Two-way Radios.....5-5
5-2	Example of an Intercom5-13
5-3	Examples of Emergency Call Boxes5-20
5-4	Indoor (left) and Outdoor (right) Digital Signage Boards5-37
5-5	Diagram of Data Transmitted to Receivers via Datacasting.....5-42
7-1	Various Components of a Visitor Database System7-18
7-2	How Tip Lines Work7-32
8-1	Security Cameras Usage and Trending in Combined, Public, and Private Schools8-4
8-2	Analog CCTV System8-6
8-3	IP Camera and Network8-7
8-4	Notional Gunshot Detection System Architecture.....8-18
8-5	RFID-based Tracking Inside a School.....8-24
8-6	Notional GPS Bus Tracking System.....8-25
8-7	Fixed-Wing UAV and Rotary Blade Quadcopter.....8-31
9-1	Examples of Personnel and Baggage Screening Areas’9-3
9-2	xample of an X-Ray Baggage Screening System.....9-10
10-1	Handle on Back of a Bullet-Resistant Whiteboard10-4
10-2	Protective Blankets10-5

LIST OF ILLUSTRATIONS (CONTINUED)

		Page
10-3	Bullet-Resistant Clipboard.....	10-5
10-4	Examples of Translucent Window Films and the Effect on the Ability To See Details Through the Film.....	10-12
12-1	Types of Technologies Covered in Federal and State Statutes and Regulations	12-14
12-2	Map of State Statutes and Regulations Requiring School Safety Plans or Specific Technology	12-15
12-3	Number of Articles Covering School Safety and Technology from 2010 to 2015 in Selected U.S. Newspapers.....	12-23
12-4	Technology in Context of School Safety in Major U.S. Newspaper Articles 2010 to 2015 Among Articles that Mentioned any Technology (N = 102)	12-23
12-5	Contextual Messages About Technology Use in Major Newspaper Coverage of School Safety from 2010 to 2015, Overall (N = 168)	12-24

This page intentionally left blank.

LIST OF TABLES

	Page
2-1 FEMA-defined Threats	2-9
2-2 Likelihood Scale.....	2-10
2-3 Consequence Scale	2-12
3-1 Access Control Devices – Technology Impact Summary	3-2
3-2 Examples of Lock Types.....	3-5
3-3 Lock Function Description Summaries and Codes	3-6
3-4 Technical Specification Considerations for Locks	3-8
3-5 Lock Cost Considerations	3-10
3-6 Lock Vendors.....	3-11
3-7 Advantages and Disadvantages of Specific Fencing Materials.....	3-14
3-8 Fencing Cost Considerations	3-16
3-9 Fencing Vendors.....	3-17
3-10 Examples of Personnel Control Devices.....	3-18
3-11 Advantages and Disadvantages of Turnstiles and Man-Traps	3-20
3-12 Estimated Purchase and Installation Costs for Turnstiles and Man-Traps.....	3-23
3-13 Man-Trap and Turnstile Cost Considerations.....	3-23
3-14 Turnstile and Man-Trap Vendors	3-24
3-15 Examples of Vehicle Barriers.....	3-26
3-16 Vehicle Barrier Cost Considerations.....	3-31
3-17 Vehicle Barrier Vendors	3-32
3-18 Bullet-Resistant Doors and Coverings Cost Considerations	3-38
3-19 Bullet-Resistant Door and Covering Vendors.....	3-38
3-20 Bullet-Resistant Windows and Films Cost Considerations	3-45
3-21 Bullet-Resistant Windows and Films Vendors	3-45
3-22 Comparison of Features of Various Types of Lockdown Devices.....	3-51

LIST OF TABLES (CONTINUED)

	Page
3-23 Lockdown Device Cost Considerations	3-54
3-24 Lockdown Device Vendors	3-54
3-25 ID Card Cost Considerations.....	3-59
3-26 ID Card Vendors	3-60
4-1 Alarms and Sensors – Technology Impact Summary	4-2
4-2 Examples of Motion Sensors.....	4-4
4-3 Technical Specification Considerations for Motion Sensors	4-8
4-4 Motion Sensor Cost Considerations.....	4-11
4-5 Motion Sensor Vendors	4-12
4-6 Examples of Photoelectric Beam Sensors	4-13
4-7 Technical Specifications for Photoelectric Beam Sensors.....	4-16
4-8 Photoelectric Beam Sensor Cost Considerations	4-18
4-9 Photoelectric Beam Sensor Vendors.....	4-19
4-10 Technical Specifications for Open-Door Sensors	4-22
4-11 Open-Door Sensor Cost Considerations.....	4-25
4-12 Open-Door Sensor Vendors	4-26
4-13 Examples of Alarm Types	4-27
4-14 Technical Specifications for Duress Alarms.....	4-30
4-15 Duress Alarm Cost Considerations.....	4-34
4-16 Duress Alarm Vendors.....	4-35
5-1 Communications – Technology Impact Summary.....	5-2
5-2 Radio Cost Considerations	5-11
5-3 Two-Way Radios Vendors	5-12
5-4 Intercom Cost Considerations.....	5-18
5-5 Intercom and PA System Vendors.....	5-19

LIST OF TABLES (CONTINUED)

	Page
5-6	Emergency Call Box Cost Considerations5-23
5-7	Emergency Call Box Vendors.....5-24
5-8	Telephone Systems Cost Considerations5-29
5-9	Telephone Systems Vendors5-29
5-10	Emergency Notification System Cost Considerations5-33
5-11	Emergency Notification System Vendors5-34
5-12	Bullhorn Cost Considerations.....5-36
5-13	Bullhorn Vendors5-36
5-14	Digital Sign Cost Considerations.....5-40
5-15	Digital Sign Vendors5-40
5-16	Datacasting Cost Considerations.....5-45
5-17	Datacasting Vendors5-45
6-1	Lighting – Technology Impact Summary6-2
6-2	Examples of Indoor Light Bulbs6-3
6-3	Indoor Security Lighting Cost Considerations6-8
6-4	Indoor Lighting Vendors.....6-9
6-5	Examples of Outdoor Light Bulbs6-9
6-6	Minimum Lighting Levels for Schools.....6-14
6-7	Ten-Year Operational Costs of Commonly Deployed Outdoor Lighting Technologies6-16
6-8	Outdoor Security Lighting Cost Considerations6-16
6-9	Outdoor Lighting Vendors.....6-17
7-1	Software Applications Impact on FEMA Mission Areas7-2
7-2	Security Planning Tools Cost Considerations7-8
7-3	Security Planning Tools Vendors.....7-9
7-4	PSIM Features and Specifications7-12

LIST OF TABLES (CONTINUED)

	Page
7-5 PSIM Cost Considerations	7-15
7-6 PSIM Vendors.....	7-16
7-7 Violence Prediction Software Vendors	7-18
7-8 Visitor Database Checks Cost Considerations	7-22
7-9 Visitor Database Checks Vendors.....	7-23
7-10 Social Media Monitoring Cost Considerations	7-29
7-11 Social Media Monitoring Vendors.....	7-30
7-12 Tip Line Cost Considerations	7-34
7-13 Tip Line Vendors.....	7-35
8-1 Surveillance Systems – Technology Impact Summary	8-2
8-2 Common Camera Types	8-10
8-3 Camera Cost Considerations	8-15
8-4 Surveillance Camera Vendors	8-16
8-5 Gunshot Location System Cost Considerations.....	8-21
8-6 Gunshot Location System Vendors	8-22
8-7 Location Tracking System Cost Considerations.....	8-28
8-8 Student Location System Vendors	8-29
8-9 UAV Cost Considerations	8-34
8-10 UAV Vendors	8-35
9-1 Weapons Detection Systems – Technology Impact Summary.....	9-2
9-2 Personnel Weapons Detection Systems Cost Considerations	9-9
9-3 Personnel Weapons Detection Systems Vendors	9-10
9-4 Baggage Screening Cost Considerations	9-15
9-5 Baggage Screening Vendors.....	9-16
10-1 Personal Protection Technologies – Technology Impact Summary	10-2

LIST OF TABLES (CONTINUED)

	Page
10-2	Bullet-Resistant Shields Cost Considerations.....10-9
10-3	Bullet-Resistant Shields Vendors10-10
10-4	Privacy Window Film Cost Considerations.....10-15
10-5	Privacy Window Film Vendors10-16
11-1	Candidate School Districts and Their Attributes11-4
11-2	District 1 Demographic Distribution11-6
11-3	Implementation Aspects of Surveillance Cameras in District 111-8
11-4	School Safety Technologies in Use in District 1.....11-10
11-5	District 2 Demographic Distribution11-14
11-6	School Safety Technologies in Use in District 2.....11-18
11-7	District 3 Demographic Distribution11-22
11-8	Implementation Aspects of PSIM in District 311-23
11-9	School Safety Technologies in Use in District 3.....11-26
11-10	Implementation Aspects for Technology at BIE Schools.....11-33
11-11	School Safety Technologies at BIE Schools11-34
12-1	U.S. Federal and State Statutes and Regulations on School Safety12-6
12-2	Federal and State Statutes and Regulations Regarding School Safety in the United States.....12-20
13-1	Security Technology13-18

This page intentionally left blank.

EXECUTIVE SUMMARY

BACKGROUND AND OVERVIEW

According to the National Center for Education Statistics (NCES), the total victimization rate at schools has declined 82% over the past two decades, from 181 victimizations per 1000 students in 1992 to 33 victimizations per 1000 students in 2014. The NCES also indicates that in 2013, fewer than 1.5% of students ages 12 to 18 reported violent or serious violent victimization at school during the previous 6 months.¹ Although schools are generally safe in the United States, rare incidents of extreme violence at schools in the United States and abroad garner public and political scrutiny and a call to assess ways to effectively secure classrooms and campuses. Incidents like those at Columbine High School in 1999 and Sandy Hook Elementary School in 2012, as well as other instances of crime and violence in schools, have sparked a rapid increase in the use of technology to ensure the safety and security of Pre-Kindergarten (Pre-K), elementary, middle, and high schools.

In 2014, the U.S. Congress appropriated \$75 million to improve school safety and allotted targeted funding to the U.S. Department of Justice's National Institute of Justice (NIJ). In response, NIJ launched the Comprehensive School Safety Initiative to conduct scientific research and evidence-based studies that build knowledge of effective means to increase school safety nationwide. NIJ's research interests included the impact of embedding law enforcement professionals or other security personnel in schools, the effects of school discipline policies, the impact of threat assessment approaches currently being used in schools, the approaches for improving school climate and culture, and the impact of school safety technologies and their impact on students' perception of safety. In addition, NIJ specifically allocated funding to enhance data collection about school safety and to conduct two assessments of technology and school safety—this effort focusing on how technology is used today to prevent violence in schools and a separate effort assessing technology needs of the future.²

Under cooperative agreement, NIJ tasked the National Criminal Justice Technology Research, Test and Evaluation (RT&E) Center at Johns Hopkins University to undertake a comprehensive assessment of how technology is currently used in the United States and in other countries to prevent and respond to criminal acts of violence in K-12 schools, both public and private. As part of the congressionally directed Comprehensive School Safety Initiative, the RT&E Center endeavored to accomplish the following objectives regarding school safety and security technologies:

- Identify technologies currently being used in K-12 schools to prevent, respond to, and mitigate criminal acts of violence.
- Identify how the technologies are being used (i.e., purpose, policy, and practice).
- Identify what is known about the efficacy of those technologies.
- Identify factors such as laws, policies, regulations, and costs that affect deployment and employment of technologies.
- Provide reports and other information to NIJ for dissemination to the various constituents that play a role in safety and security in schools.³

¹ Zhang, A., Musu-Gillette, L., and Oudekerk, B.A. (2016). *Indicators of School Crime and Safety: 2015* (NCES 2016-079/NCJ 249758). NCES, U.S. Department of Education, and Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, Washington, DC.

² U.S. Department of Justice, Office of Justice Programs, NIJ (May 2014) "Comprehensive School Safety Initiative Report."

³ Ibid

The resulting report, entitled “A Comprehensive Review of School Safety Technologies,” is intended to be used by a range of audiences, including school administrators, security directors, principals, and others. It features four research components—a literature review, a technology review, case studies, and a legal review. It examines the technologies currently being used, how they are used, how those technologies were chosen, and how well they are working. By providing this context, school officials can make informed decisions about technology choices that can increase the safety of school children, faculty, and staff.

LITERATURE REVIEW

The literature review provides perspective on school safety and security technology. It features research from the academic community and practitioner community in the United States and internationally. In addition, research was compiled regarding risk assessment and security technology in the school community. The literature review is intended to provide an overview. Research related to a specific technology is included in the relevant technology chapter, rather than in the literature review.

UNITED STATES LITERATURE REVIEW

Drawing on available academic literature and other published sources, the current understanding of the use of technology to prevent and respond to acts of criminal violence in Pre-K to grade 12 schools was assessed.

The vast majority of the literature corroborates the conclusion that public and private schools are safe.⁴ Whether located in urban, suburban, rural, or tribal communities, the students, teachers, staff, and guests in schools experience few serious crimes. Incidents such as the heinous attacks at Sandy Hook Elementary in Newtown, CT, and in other locales (e.g., Moses Lake, WA; Pearl, MS; Paducah, KY; Jonesboro, AK; and Littleton, CO) are rare incidents that are the exception rather than the rule; however they tend to dominate almost every conversation about school safety and generate a societal belief that schools are potentially dangerous places.⁵

Much of the literature on school safety technology goes beyond security and prevention of criminal acts and aberrant behavior. It encompasses fire prevention and response, healthcare, an array of environmental issues (e.g., air quality, hazardous materials, waste disposal, pest management), roadways of ingress and egress (external to the school facility), vehicle and traffic control, and the relationship of technology and the school environment to academic achievement.

Among the most notable technology trends uncovered in the literature review are the following:

- Cloud-based systems and services
- Connection of security systems to mobile devices
- Enhanced imaging and high-resolution cameras
- Integrated hardware
- Integrated software
- Social media use and monitoring
- Wireless devices

⁴ Perumean-Chaney, S. E., and Sutton, L. M. (2013) “Students and perceived school safety: The impact of school security measures.” *American Journal of Criminal Justice*, 38(4), 570–588

⁵ Toppo, G. (2013) “Schools safe as ever despite spate of shootings, scares.” Retrieved 24 September 2015 from <http://www.usatoday.com/story/news/nation/2013/11/13/school-violence-security-sandy-hook/3446023/>

Integrating technology—physical security, software, internal communications and monitoring, and shared information—will continue to be an area for development and expansion in the future.

Some schools with few problems or threats are well equipped with safety and security technology, whereas other schools with recurring crime and related needs have little or none of the desired safety and security technology. Although some of the literature references the importance of “fit” and meeting the specific needs of each school, there is limited evidence-based information on how to conduct a technology assessment to address such fit.

In addition, there is minimal information concerning analytical processes applied to decision-making about school safety and security technology. Specifically, there is little information on the technology choices and how many alternatives were available to school administrators at the time they made decisions to purchase or apply specific safety and security technology.

Many of the activities that schools undertake to promote safety and prevent problems, including use of technology, have not been evaluated. There is limited and conflicting evidence in the literature on the short- and long-term effectiveness of school safety technology. Lastly, the literature on school safety technology tends to focus on the types of technology and people’s perceptions of it rather than the actual efficacy of the technologies.

Responsibility for controlling technology is assumed by state, regional, and local school systems and, often, individual schools. Research on school safety technology has been inhibited by inconsistencies in the available data and lack of information on planning, policy and regulation, types of technology, and methods of assessment.

INTERNATIONAL REVIEW

Focusing on technology-based approaches used worldwide, the international review reflects available academic literature and other published sources to describe what is known about the use of technology in a sampling of countries around the world.

Violence and the threat of violence have affected and continue to affect communities in almost every nation.⁶ Although preventing and managing violence in schools is a goal of nations around the world, security initiatives vary greatly, as do data on the types of technology used and assessment of the applications.^{7,8} The literature on use of security technology and its outcomes, particularly in developing and underdeveloped nations, is slight, and much of it is based on media reports, local and regional data collection, and anecdotal information.

The worldwide concern for school safety has not evolved into a common commitment to the use of security-related technology or development of standards to guide that use. Application of such technologies is inconsistent due, in part, to the differences in and fragmentation of systems, often in the same state or nation. In most nations, there is no central authority that dictates type or use of safety and security technology or assesses its impact on preventing and intervening in violence.

⁶ Akiba, M., LeTendre, G. K., Baker, D. P., and Goesling, B. (2002) “Student victimization: National and school system effects on school violence in 37 nations.” *American Educational Research Journal*, **39**(4), 829–853.

⁷ Brunner, J. M., and Lewis, D. K. (2008) *Safe & Secure Schools: 27 Strategies for Prevention and Intervention*. Corwin Press.

⁸ Robinson, M. (2014) “A five-step approach to solving school security.” Retrieved from <http://www.ifpo.org/resource-links/articles-and-reports/school-security-training/a-five-step-plan-to-solving-school-security/>.

The most basic forms of school security technology—the use of door locks, lighting, and alarms—are not universal. In developing and underdeveloped nations, as well as some developed countries, the struggle to obtain the basic essentials for learning such as teachers, teacher’s aides, student healthcare, books, paper, computers, and room lighting take precedence over security-related technology. Fire alarms and fire suppression technology also take precedence over security technology.

Generally, the better-funded schools in developed and some developing nations tend to use some or all of the most common types of school security technology. These include computer and social media alerts, identification card or biometric access control, panic and alarm buttons, scans of social media, use of mass messaging software for prevention and response, video surveillance, and visitor management.⁹

There is no global clearinghouse or database that provides collective information on school safety. A 2007 Eastern European study conducted by UNICEF and the Commonwealth of Independent States asserted that global data on school safety are lacking and that information gathering in many nations is dependent on the institutional memory of teachers and principals.¹⁰

Schools in much of the world are part of a fragmented system or no system at all. Decisions, including those related to security and the purchase and use of technology, are made independently of a central authority and often without national, state, or regional guidelines. In many locales around the world, community leaders (political, military, and tribal) dictate decisions for schools regarding technology and other resources absent input from educators or security experts.

Schools in developed and less-developed areas focus on preventing different events. Those in developed nations focus heavily on preventing and intervening in catastrophic events, whereas in less-developed and poor nations, schools tend to focus on preventing culturally tolerated violence. In many nations there are no fiscal resources and infrastructure to support basic or advanced school security technology. Applying a “developed nation standard” of school safety and security to schools worldwide is ineffective.

SCHOOL SAFETY AND SECURITY TECHNOLOGY IMPLEMENTATION PLANNING

By implementing a security technology, school officials usually intend to reduce their exposure to risk in their district, building, or location. The application of risk management to school safety technology decisions is explored through a review of academic and professional literature.

In schools, fear of violence and of legal liability are two arguments that school district administrators use to show security technology is worth the expenditure. There is a large volume of general literature on risk assessment and planning tools for schools. Numerous articles call for schools to conduct risk assessments, and a large number of online sites offer risk assessment toolkits. The scholarly literature is extensive in addressing the need for risk assessment in schools and commonly cites the components of risk assessment tools and processes; however, few sources evaluate these tools and processes.

Decisions about whether to invest in school security technology for a school or school district are complex and must take into account various logistical, economic, and political factors. Many choices

⁹ Winske, C. (2015) “Seven solutions to secure school campuses.” Retrieved from http://www.securitysales.com/article/7_solutions_to_secure_school_campuses

¹⁰ Richardson, D., Hoelscher, P., and Bradshaw, J. (2008) “Child well-being in Central and Eastern European countries (CEE) and the Commonwealth of Independent State (CIS).” *Child Indicators Research*, 1(3), 211–250

about the technology selected, however, may be made with incomplete information or with information that is influenced more by political or reactionary consideration than by local conditions.¹¹

A comprehensive evaluation should take place before a technology solution is chosen. The evaluation could draw on a number of approaches, including user surveys and safety audits, risk management, analysis of alternatives, and other tools. Districts and schools with chronic violence or small budgets should not take the same approach as those where violence is rare or budgets are large.

Using a risk assessment process, schools and districts can select the most effective mitigation measures to achieve a desired level of protection against a wide range of threats. Generally, a district or school needs to understand the likelihood that a specific threat or hazard will occur and the effects it likely will have, including the severity of the impact, the amount of time the school will have for advance warning to students and staff about the threat or hazard, and how long any disruption may last.¹²

Acquiring security technology alone cannot solve all school security problems; it must be integrated into broader prevention and intervention measures, ranging from security and emergency response plans to crisis response drills to a positive school climate. Choosing the right device or devices is a complex and recurring task. Making effective choices requires decision makers to match goals and objectives with threats, consequences, and vulnerabilities to justify the selection of a technology or suite of technologies. A collaborative planning effort, including a strong planning team, can be an effective way to gain acceptance and buy-in.

TECHNOLOGY REVIEW

To accomplish the study objectives, basic and advanced school security technology including physical security technologies, information technologies, and social media technologies were examined in depth. Specific technologies, such as lighting, locks, alarms, access control, communication, cameras, social media monitoring, risk assessment, and emergency notification, were grouped with similar technologies based on their intended use. These groups are:

- Access control
- Alarms and sensors
- Communications
- Lighting
- Software applications
- Surveillance
- Weapons detection
- Other technology systems that do not fit into the preceding categories

A high-level summary of the findings from each technology group is included next.

¹¹ Hevia, J. (2013). *Impediments to U.S. Educational and Public Institutions Ameliorating the Mass Shooting Epidemic with Effective State-of-the-Art Security Solutions and the Introduction of a School Access-Control Vulnerability Index (S.A.V.I.) Audit and Certification Process, As a Solution*. Napco Security Technologies, Inc.

¹² U.S. Department of Education (2013) Office of Elementary and Secondary Education, Office of Safe and Healthy Students. *Guide for Developing High-Quality School Emergency Operations Plans*.

ACCESS CONTROL

Access control devices prevent or otherwise control physical access to school property, people, and resources. These devices are some of the most widely used for school security and safety. They are used to keep doors closed when necessary, direct pedestrian flow within schools, maintain control of school property boundaries, and direct and control vehicle access into and around school property. Examples include locks, fences, vehicle barriers, turnstiles, bullet-resistant doors and window coverings, and lockdown devices. In addition to preventing entry to school grounds or buildings, these devices are used to prevent theft and vandalism, help ensure school visitors are more easily accounted for, and ensure specialized equipment and other items are safely secured.

Identification cards, when issued and worn, are also a form of access control that ensures individuals on school property are easily identified and visitors are distinguishable from students, faculty, and staff. If used in conjunction with electronic locks, they can also manage access to specific locations, facilities, and/or functions.

Electronic access control systems are rapidly changing as a result of advances in technology. New capabilities such as biometric reader lock capabilities are entering the marketplace. Technologies, particularly those with an electronic and software component, can be integrated with other security systems like sensors and cameras to provide more robust school safety capabilities. School officials should carefully consider the potential technological advancement of these systems and, when possible, accommodate current and future system integration and upgrade possibilities.

ALARMS AND SENSORS

Sensors and alarms facilitate the notification and engagement of school and law enforcement officials in the event of a crime or emergency. Due to the nature of this report, however, items like fire alarms are out of scope. A sensor is “a device that responds to a physical stimulus (e.g., heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse as a measurement or operating a control.”¹³ Alarms create an alert, based on input—from a sensor or human—indicating the presence of an intruder.¹⁴

When used in conjunction with an alarm panel and appropriate rule set, sensors such as motion sensors, open-door sensors, or open-window sensors can automate the detection of intruders in the school environment. Alarms created by a panic button, badge alarm, silent alarms, or alarm panel facilitate the notification of school or law enforcement personnel.

Alarms and sensors, like technology generally, are rapidly changing and improving. Consideration should be given to capabilities, limitations, replacement and maintenance costs, and policy impacts prior to installing or upgrading these systems. System integration is an important consideration because these types of systems can be integrated with other security systems (like access control or surveillance systems) to provide more robust school safety capabilities.

Some smart cameras are also marketed as motion-sensing devices. These smart cameras use image processing to detect what is happening in an image and analyze the actions of people in the image.

¹³ <http://www.merriam-webster.com/dictionary/sensor>

¹⁴ Alarms should not be confused with sirens, which create a sound when activated.

Sensors also exist to detect chemical, biological, and radiological/nuclear hazards. Although these hazards are very real for schools in active war zones around the world, U.S. schools have not yet confronted these types of threats.

COMMUNICATIONS

Communications devices are designed to facilitate or monitor the communication of personnel within the school or stakeholders outside the school such as first responders, administrators, or the surrounding community.

Communication is one of the most vital capabilities for school officials and first responders in the event of an act of criminal violence or natural disaster. One-way communication devices, such as digital signs and public address systems, and two-way communication devices, such as radios, telephones, and intercoms, are widely used in the school community. In one-way communications, a message is transmitted or broadcast with no means for acknowledgment or response. With two-way communications, messages may be exchanged between two or more parties.

Communications technologies are generally dual use, in that they are primarily designed for day-to-day, non-emergency operations but essential for emergency operations. The benefit of dual-use technology is increased attention to training and maintenance, thus making it more likely to be available and to be used effectively in the event of an emergency.

For school safety purposes, communications technologies are most important during and after an event. As with other technologies, integrating communications with the overall school safety plan increases the effectiveness of these technologies across all areas. In addition, schools should coordinate with first responders when making decisions about communications technology to ensure the systems can interoperate or integrate as needed.

LIGHTING

Generally, security lighting creates a deterrent to intrusion, vandalism, and burglary. Lighting also enables other technologies, such as cameras, to work more effectively.

Motion sensors can be used in conjunction with indoor lighting to detect when a person has entered the room. This allows the lights to be turned on when movement is detected, and then turned off automatically when motion has not been detected for a set period of time.

Because of their long life and reduced power consumption, light emitting diode (LED) type bulbs are increasingly being used in security lighting applications.¹⁵

SOFTWARE APPLICATIONS

Software applications have the ability to help school staff analyze and combine electronic data and resources to improve school safety. Applications include security planning tools, physical security information management systems, violence prediction software, visitor database checks, mental and public health information sharing, tip lines, and social media monitoring. The common role for all of these technologies is detection or mitigation of security risk.

¹⁵ Swedberg, C. (2012) "The LED Inevitability." *Electrical Contractor*. Retrieved from <http://www.ecmag.com/volume/december-2012-lighting-special-report>.

These tools help identify risks, assist in planning, and enable the school or school district to recognize emerging security challenges. Software applications generally have the potential to help school staff prevent, protect, and recover from acts of criminal violence. Electronic planning tools have the same benefits as a manual process—building or strengthening relationships—and ease the process of maintaining plans. Once created, however, school officials should train and exercise the plans regularly.

Another technology whose acquisition is trending upward is visitor database applications. By using a visitor's driver's license or other state-issued identification, these systems can screen for registered sex offenders, domestic violence offenders, and other individuals of interest.

Some software also can provide situational awareness for schools. Integration, or the desire for increased integration across security technologies, is a growing trend. In this way, school officials mitigate risks with a combination of capabilities.

By extending school security into cyberspace, where students spend a significant amount of their time, social media monitoring technology employs tools “to proactively prevent, intervene and [watch] situations that may impact students and staff.”¹⁶ Specified alerts generated by software that monitors Facebook, Twitter, Snapchat, and other social media can cue school officials to intervene with students to prevent a suicide, stop bullying, or protect students from other possible violence. Software applications like mental health information sharing and violence prediction software are not mature in the school safety market, but with advances in technology they may have great promise for reducing risk to the school or district.

Many factors have to be weighed in this investment—including cost, unique school demographics and environment, and expected effectiveness in a given school district—but these capabilities are increasingly more relevant to the total picture of school security.

SURVEILLANCE

Surveillance systems allow school personnel and responders to monitor and better understand emergency situations as they arise. Items such as surveillance cameras, gunshot-detection technology, radio frequency identification (RFID) system and global positioning system (GPS) location tracking, and unmanned aerial vehicles are used to monitor students, school staff, school grounds, and school assets.

Public and private schools deploy thousands of security cameras; this technology is the second most-used security measure^{17,18} in public schools. Their value to security is heavily dependent on the way they are deployed:

- Camera feeds can be transmitted to a monitor with an individual assigned to watch the video feed. When a behavior is observed, security staff can immediately be sent to the location of the incident.

¹⁶ Griffin, A. (2015) “Schools use social media monitoring software to watch students.” *The Independent*. Retrieved from <http://www.independent.co.uk/life-style/gadgets-and-tech/news/schools-use-social-media-monitoring-software-to-watch-students-10288541.html>.

¹⁷ U.S. Department of Education, NCES, Schools and Staffing Survey (SASS). (2011–2012) “Public School Principal Data File” and “Private School Principal Data File.”

¹⁸ In both public and private schools, controlling access to school buildings during school hours was the number one safety or security measure used. In private schools, enforcing a strict dress code, the wearing of uniforms, and controlling access to school grounds preceded camera deployment in importance.

- The camera feed can be transmitted to a monitor that does not have a dedicated observer. This configuration may have value in deterring undesirable behavior. Stored video footage may aid in identifying perpetrators and verifying testimony;
- Systems employing video analytics capabilities provide automatic detection and alerting features. A video feed can be highlighted for further observation by security staff so they can select an appropriate response.

Analog camera systems are being replaced with newer digital units. These more advanced cameras are easier to integrate with other security systems and they permit the use of video analytics capabilities.

Gunshot location systems, deployed in only a handful of schools, detect a gunshot, identify the gunshot's location, automatically generate an alert, and send the alert to first responders and others on a predetermined notification list. By detecting and alerting almost instantaneously following a gunshot, this technology allows students, staff, and other building occupants to immediately take protective actions.

Some schools use RFID or GPS technology to track the movement of students and buses. These two technologies are not mutually exclusive and can be combined (e.g., while tracking students in a school bus on a field trip). By notifying school authorities when students are not where they belong, the likelihood is reduced of leaving students on an empty school bus at the end of a route, in an empty building at the end of a school day, or at a field trip site. The technology can also alleviate fears of serious criminal incidents, such as child molestation or kidnapping, if children miss their school bus in the afternoon, miss their stop, or get off at the wrong location.

WEAPONS DETECTION

These systems detect weapons concealed on persons or in their belongings. Usually they are intended to detect large or small quantities of metallic, organic, or explosive objects such as firearms, knives, and incendiary devices.

Installing metal detectors and x-ray screening devices requires careful thought about system footprint and throughput, impacts to traffic patterns, types of weapons detected, system safety, and false alarm rates. In addition, these systems can be costly to purchase and maintain, are reliant on ongoing training, and require careful policy considerations due to privacy rights during screening.

There are other potential screening technology types available and in development for the purpose of weapons detection such as millimeter wave personnel screening systems. These types of systems may become attractive to schools as the technology matures. Because of the dynamic nature of the weapons detection market and school security technology market, school officials should periodically review available and emerging systems to identify those that might be best suited for their school applications.

OTHER TECHNOLOGY SYSTEMS

There are several school safety technology options that are difficult to categorize and are narrowly focused on active-shooter prevention. These include bullet-resistant objects—clothing, blankets, whiteboards, or other types of shields—that are intended to protect one person from an armed intruder. More generally, film applied to interior or exterior glass prevent intruders from viewing the interior of the building or classroom and some can make the windows bullet resistant.

School officials should carefully weigh capabilities against factors like cost per person or per window, storage locations and access, multi-use applicability, and installation time when considering these types of devices.

CASE STUDIES

The case studies provide examples of school safety technologies deployed in four different school environments. This snapshot in time contributes context to the use of school safety technologies, their implementation, and considerations affecting implementation.

Because of the small sample size, it would be inappropriate to generalize the case study data to a larger population. Nevertheless, useful observations may be made. Participants all mentioned an increasing commitment in the school community by students, parents, teachers, administrators, and staff toward safer, more secure schools, and all of them use technology in varying degrees to make their schools safer. For example, commitment to ensuring exterior doors remain closed during school hours was a point of emphasis. A desire for increased understanding, or situational awareness, of the security in the districts, mainly through technology, was expressed. Communications were consistently highlighted as very important. Multiple districts were also interested in tip lines and basic locks, indicating that basic technologies are recognized as a valuable foundation for more high-tech forms of security technology.

Budget constraints and political commitments frequently require tradeoffs between security and school operations. Based on the information obtained from the case studies, however, obtaining technology to make schools safer will continue to be a priority.

The districts all stressed that technology, used in isolation, is not a panacea. There is hard work—from strategic and emergency planning to relationship building to drills—that must accompany the deployment of any technology. Each district provided anecdotes suggesting technology made their school districts safer, but none could point to data or metrics that demonstrated an evidence-based relationship between the deployment of safety technology and prevention or reduction of acts of criminal violence. Nonetheless, each district had a “wish list” of additional technology measures that they desired to implement.

Having a champion who is interested in school safety, knowledgeable about technology implementation, and takes an active leadership role in promoting school safety technologies seems to have been one of the foundations of successful technology acquisition and integration.

LEGAL REVIEW

Because laws and regulations affect some decisions regarding the acquisition and implementation of technologies for school security, the laws and regulations of all 50 U.S. states, the U.S. territories, and the Federal Government were reviewed. They can compel or prohibit specified behaviors, require certain designs of the built environment, and mandate or limit the use of technologies in schools for the protection of those within them.

With few exceptions, the statutes and regulations do not delineate specifically what school districts *must* do, but they do provide a broad framework for what they are *allowed* to do. Results from the accompanying media analysis suggest that, within this broad framework, schools are taking actions to protect the safety of their students and staff, often using technology such as video surveillance technology, new locks, and other access control technology. Thus, although the law may seem vague, schools are proactively implementing planning and technology-based safety measures.

Of the five Federal statutes identified, three mentioned technology; of those three, two require the use of technology. Laws at the Federal and state levels, in general, create an obligation for schools to have safety plans, but with few exceptions they do not specify the types of technology allowed or required. State-level statutes and regulations offer little guidance or specifics as to how to ensure the safety of the school or the role that technology should play in school safety. One possible reason for this is that technology develops quickly and is always changing, whereas law generally lags considerably behind the available technology, and the process by which new laws or regulations are created is slow by comparison.

Forty-nine states and territories have passed laws that require the adoption of a school safety or security plan. More specifically, the law in 23 of these jurisdictions prescribes the application of some type of technology as part of a comprehensive school safety, crisis response, or emergency preparedness plan. In jurisdictions that have legislated the use of specific technologies, the requirement for technology is generally only one element of a more comprehensive school safety or crisis response plan. When technology is prescribed, the focus tends to be on weapons detection, access control, communications, and surveillance technologies.

Only two jurisdictions specifically limit the use of security-related technology with regard to school safety, and these legislative restrictions are narrowly tailored to address Fourth Amendment privacy concerns.

Among the 17 state regulations identified, 5 specify a particular category of technology that must be employed as part of school safety standards and security procedures.

A few states have contemplated the need for guidance with respect to a violent or traumatic event occurring on a school bus and have included provisions in their school safety laws to address technology on buses.

News media coverage provides an additional lens through which the team examined the use of technology for school safety and the public attitudes about safety measures in schools. Access control technologies were the most frequently discussed in news coverage about school safety (74% of articles), followed by surveillance technologies (63% of articles), communications technologies (26% of articles), alarms technologies (24% of articles), and weapons detection technologies (21% of articles). Cyber systems and lighting technologies were discussed the least (10% and 4% of articles, respectively).

Law, in all of its forms, can be a useful tool in creating duties and providing guidance regarding the use of technology to best ensure safety in the country's K-12 schools. Given the Federal system of law in the United States, by which much authority is left with the states to protect the health and safety of their citizens, one would expect to find wide variations in the approaches states have taken regarding technology in schools. Overall, however, states have provided policies that, in broad terms, set the clear expectation that technology can and often should be deployed, with limited restrictions involving the safeguarding of privacy rights, to enhance the safety of students, faculty, and staff in the nation's schools.

CONCLUSION

There is no universal school safety solution—no one technology will solve all school safety and security issues. The sheer number of schools and school districts across the country—with different geography, funding, building construction and layout, demographics, and priorities—make each one different. Technology that is useful in one school district may not be appropriate for a neighboring district; for that

matter, neighboring schools in the same district will often have different requirements. It is important to recognize these differences when choosing technologies. It is also important to consider how a new or upgraded technology will work with other technologies and existing safety plans. For some situations, layering multiple technologies may be required to achieve the desired effect on school security.

When considering acquiring, replacing, or upgrading security it is important that schools assess their current situation, including the risks and issues that need to be addressed, and then carefully determine appropriate solutions that meet those needs while accommodating any regulatory or budgetary constraints.

Methods for evaluating safety and security technology are lacking in two discrete areas:

- Prior to selecting and acquiring technology, evaluation is sometimes ad hoc or extremely limited. In some cases, technology is selected to assuage the anxiety brought on by recent news stories or in response to a flood of funding.
- Quantitative methods or metrics to evaluate the effectiveness of a given technology for reducing or eliminating acts of criminal violence were not found. Anecdotal evidence was provided that describes reductions in criminal acts of violence after certain technologies were installed. In addition, evidence that “sophisticated” or expensive technologies are better or more effective than “simpler” or less expensive technologies is lacking.

Serious incidents seem to stimulate increased interest in safety and security. If horrific enough, these incidents can lead to increases in funding with a short spending window. This curbs the ability of districts to conduct even limited evaluation and frequently results in the purchase of technology to demonstrate a strong commitment to “doing something.”

Some of the most sophisticated technologies being deployed are demonstration projects conducted by vendors deploying their solution into a selected school. In most cases, these demonstrations did not plan for or produce metrics to show the effectiveness of the technologies after installation or to compare the effectiveness with other technologies. Technologies, particularly those based on computers or information processing devices, tend to develop rapidly if there is a proven benefit and demand.

This report represents one data point in time. Because the safety and security field moves rapidly, it should be used as a foundation for further research prior to making any final decision.

Chapter 1. INTRODUCTION

Steven R. Taylor, MPA, and Sheldon F. Greenberg, PhD

Over the past decade electronic security technology has evolved from an exotic possibility into an essential safety consideration. Technological improvements are coming onto the market almost daily, and keeping up with the latest innovation is a full time job. At a minimum, a basic understanding of these devices has become a prerequisite for well-informed school security planning.

—National Clearinghouse for Educational Facilities
National Institute of Building Sciences, 2009

There is no panacea for stopping all targeted violence....Science and technology initiatives aimed at preventing targeted violence do show some promise over the long-term, as an aid to threat management.

—Task Force Report: Predicting Violent Behavior
Defense Science Board, 2012

1.1 PURPOSE

According to the National Center for Education Statistics (NCES), the total victimization rate at schools has declined 82% over the past two decades, from 181 victimizations per 1000 students in 1992 to 33 victimizations per 1000 students in 2014. The NCES also indicates that in 2013, fewer than 1.5% of students ages 12 to 18 reported violent or serious violent victimization at school during the previous 6 months (Reference 392). Although schools are generally safe in the United States, rare incidents of extreme violence at schools in the United States and abroad have resulted in increasing public and political scrutiny and a call to assess ways to more effectively secure classrooms and campuses. Incidents like those at Columbine High School in 1999 and Sandy Hook Elementary School in 2012, as well as other instances of crime and violence in schools, have sparked a rapid increase in the use of technology to ensure the safety and security of Pre-Kindergarten (Pre-K), elementary, middle, and high schools.

Technology can play an integral role in the prevention and mitigation of crime and other threats, ranging from inappropriate behavior to fire. A broad range of technologies is applied to improving school security and safety, including low-technology devices such as lights, doors, locks, and door pins, and, at the other end of the spectrum, metal detectors, surveillance cameras, social media, infrared detection, and sophisticated school-to-police communication systems.

This report, featuring four research components—a literature review, a technology review, case studies, and a legal review—will allow readers to gain an understanding of the current school safety technology in use, its implementation, and considerations affecting implementation. The report examines the technologies currently being used, how they are used, how those technologies were chosen, and how well they are working. By providing this context, school officials can make informed decisions about technology choices that can increase the safety of school children, faculty, and staff.

1.2 BACKGROUND

The U.S. Department of Justice's (DOJ's) National Institute of Justice (NIJ) awarded a 5-year cooperative agreement in 2014 to establish the National Criminal Justice Technology Research, Test and Evaluation (RT&E) Center at The Johns Hopkins University (JHU). The RT&E Center is a partnership of the JHU Applied Physics Laboratory and the JHU School of Education, Division of Public Safety Leadership. The primary goal of the RT&E Center is to conduct research into technologies available to law enforcement, corrections, and the courts to achieve their missions. To do so, the RT&E Center conducts tests and operational evaluations of selected technologies, provides evidence-based assessments for the criminal justice community, and assists NIJ in its effort to improve the knowledge and understanding of crime and justice issues through science.

In 2014, the U.S. Congress appropriated \$75 million to improve school safety and allotted targeted funding to DOJ's NIJ. In response, NIJ launched the Comprehensive School Safety Initiative to conduct scientific research and evidence-based studies that build knowledge of effective means to increase school safety nationwide. NIJ's research interests included the impact of embedding law enforcement professionals or other security personnel in schools, the effects of school discipline policies, the impact of threat assessment approaches currently being used in schools, the approaches for improving school climate and culture, and the impact of school safety technologies and their impact on students' perception of safety. In addition, NIJ specifically allocated funding to enhance data collection about school safety and to conduct two assessments on technology and school safety—this effort focusing on how technology is used today to prevent violence in schools and a separate effort assessing technology needs of the future (Reference 360). This report constitutes the assessment of technology currently in use to prevent violence in schools.

Schools worldwide depend on basic and advanced technology to provide and reinforce school safety and security. Recognizing this, NIJ tasked the RT&E Center, under cooperative agreement, to undertake a comprehensive assessment of how technology is currently used in the United States and in other countries to prevent and respond to criminal acts of violence in K-12 schools, both public and private. As part of the congressionally directed Comprehensive School Safety Initiative, the RT&E Center endeavored to accomplish the following objectives regarding school safety and security technologies:

- Identify technologies currently being used in K-12 schools to prevent, respond to, and mitigate criminal acts of violence.
- Identify how the technologies are being used (i.e., purpose, policy, and practice).
- Identify what is known about the efficacy of those technologies.
- Identify factors such as laws, policies, regulations, and costs that affect deployment and employment of technologies.
- Provide reports and other information to NIJ for dissemination to the various constituents that play a role in safety and security in schools. (Reference 360)

To meet these objectives, the RT&E Center team began with literature and legal reviews, including a review of existing studies, laws, and regulations; and interviews with experts in school safety from DOJ, Department of Education (DoED), state and local jurisdictions, national associations, and other significant private and public school safety initiatives. These resources helped define school safety needs and the categories of technologies to review. Research on technologies was drawn from a wide range of sources, including previous studies, government and industry literature and statistics, national associations and publications, and interviews with vendors and users of the technologies. To provide additional context, case studies were conducted on a small set of school districts.

This study did not include experimentation with specific technologies or large-scale surveys or quantitative research.

1.3 SCHOOLS

There are approximately 132,000 schools and 14,000 school districts in the United States. Of these, approximately 99,000 schools are public. There are approximately 54,876,000 students attending the nation's schools (Reference 89). Schools across the nation employ approximately 3.1 million full-time equivalent teachers. One-third of the nation's public schools are rural, serving approximately 12 million students (References 234 and 321). The term "schools" includes large city and county systems, individual school districts within the same jurisdiction, independent school taxing districts, parochial schools (ranging from large diocesan systems to schools managed by a single religious institution), private schools (nonprofit and profit-making), and others. This fragmentation makes standardization, regulation, implementation of technology, and research on school security and violence prevention difficult.

On any given day, public schools may be among the largest functioning organizations in an urban, suburban, or rural jurisdiction or region. Enrollment ranges from 2277 to 5858 students within the thousand largest high schools in the United States (Reference 235). Commonly, public schools are among the most densely populated centers of activity in any community.

While extreme or extraordinary violence in schools, such as mass casualty shootings, are rare occurrences, these events have garnered national and international attention (Reference 116). Although some schools are troubled and therefore defy the norm, data show that criminal offenses committed by people in schools, as well as those from outside schools who enter the environment, are infrequent and have declined in recent years. Whether located in urban, suburban, or rural environments, violent victimization of adults, young adults, and children in U.S. schools is rare. Data show that public and private schools are quite safe (Reference 270) and most disruption in schools is caused by disciplinary issues, some of which have also drawn national attention (References 139 and 319).

National attention to extreme acts of violence in schools increased exponentially after the mass shooting at Columbine High School in April 1999. Today, incidents such as the heinous attacks at Sandy Hook Elementary in Newtown, CT, and in other locales (e.g., Moses Lake, WA; Pearl, MS; Paducah, KY; Jonesboro, AK; and, Littleton, CO) come to the forefront in almost every conversation about school safety and have generated a societal belief that schools are dangerous places (Reference 344). In addition, many of the nation's most serious attacks in schools have occurred in small towns and rural communities that, despite popular belief, are not immune to these threats (Reference 101), such as the 2006 shooting at an Amish school in Lancaster County, PA. Despite heightened attention to events of extreme violence, safety-related concerns in schools are far-reaching and include issues such as theft, bullying, cyberbullying, vandalism, bomb threats, suicides, non-aggravated assaults, trespassing, sexual assaults and intimate partner violence, racial tension, hazing, crowd control at special events, transit and traffic safety, and more (Reference 171). Although school safety is difficult to measure, most indicators reinforce that school safety in this country has increased. Since 1992, the rate of victimization for violent and nonviolent incidents in schools has declined from 181 incidents per 1000 students to 49 per 1000 students (Reference 290).

Open access to the school environment and freedom of movement within school boundaries causes the Department of Homeland Security (Reference 308) to classify school facilities as vulnerable sites. The

degree to which school facilities should be open versus secured environments remains a subject of debate among educators and law enforcement officials.

Although research has been conducted on crime, violence, security, and the role of police in schools (References 44 and 45), little is known about why systems, districts, and schools adopt specific approaches to school safety (Reference 283). An increasing body of literature has emerged on crime and fear within and external to school facilities.

School safety and order are essential conditions for learning in all schools regardless of the environment, locale, or community demographics (Reference 77). Repeated crimes—serious and non-serious—disrupt the school environment and impede learning. Safety in schools may also be disrupted by threats, fear, hate, revenge, disagreement, and other actions and behaviors that may not rise to the level of a criminal act under the law. Research also shows that people’s perception of a safe school impacts behavior and learning (Reference 299).

1.4 APPROACH TO THE TASKS

To accomplish the study objectives, a multi-faceted approach was used. The decision was made early in the study to focus on the most widely deployed basic and advanced school security technology including physical security technologies, information technologies, and social media technologies (Reference 360). For example, specific technologies, such as lighting, locks, alarms, access control, communication, cameras, social media monitoring, risk assessment, and emergency notification, were all included. Subsequently, these technologies were grouped with similar technologies based on their intended use.

Small teams were established to research each category of technology. The members of each team were selected because of their academic and professional expertise regarding the physics, phenomenology, or operational use of the assigned technology category. Each team’s efforts were supported by the development of case studies, review of the literature, and input from practitioners. Study team members developed methods of inquiry and technology review appropriately tailored to each technology category. Generally, this included a review of open-source materials to obtain a high-level sense of the state of practice, vendor-supplied materials, existing authoritative technical documents and surveys, standards, and scholarly literature.

Weekly meetings were held with team leaders to share findings, identify obstacles, and advance research. Each team provided progress reports to the study lead. Meetings were held with current and former school principals, teachers, law enforcement personnel (including school resource officers), and subject matter authorities in school safety. Teams attended school safety conferences to learn about current trends, best practices, and vendor offerings. In addition, meetings were held with and regular updates were provided to NIJ officials.

Professional associations that are concerned with, and continue to do work on school safety and security, were contacted. Among them were the National Association of School Safety and Law Enforcement Officials, the School Safety Advocacy Council, the National School Safety Center, the National Association of Secondary School Principals, the National Association of School Resource Officers, the International Association of Chiefs of Police (a partner agency to the RT&E Center), and the Police Executive Research Forum.

Recognizing that laws and regulations might affect decisions regarding the acquisition and implementation of technologies for school security, the Johns Hopkins Center for Law and the Public’s Health reviewed the laws and regulations of all 50 states, the U.S. territories, and the Federal

Government. The members of the legal team met regularly with the other team members, and others reviewed their work.

The study was divided into several topics with team members assigned to one or more topics. Overlap was considerable and was addressed during team meetings. Study topics included the following:

- Technology implementation
- Access control
- Alarms and sensors
- Communications
- Lighting
- Software applications
- Surveillance
- Weapons detection
- Additional technologies that do not fit into the above categories

Product searches on the most widely used technologies were conducted using a variety of resources. For some topics, vendors were contacted to provide supportive information on technologies and assessments. In addition, the team focused on developing case studies and conducting a legal review (law and regulation), literature review, and international review.

1.5 LIMITATIONS

The scope of the study was partially constrained by a variety of factors including time, resources, and the volume of and disparity across school systems. These limitations prevented the team from conducting a large-scale national survey of school systems.

A major issue that arose early in the study was the inconsistency across schools and schools systems in defining security technology, particularly as it relates to the prevention of and response to violence. Some school officials do not consider basics such as locks, fencing, and lighting when discussing security technology; others focus on safety technology such as fire suppression. Many school officials blend discussion about classroom management and behavior management issues when discussing use of technology to prevent violence.

From the inception of this study, the authors recognized that technology solutions alone will not ensure the safety of schools. To be effective, technology must be incorporated into a comprehensive framework that includes non-technological interventions, extensive planning and training, and rigorous evaluation against the needs of the individual school or system. However, this study exists in the context of a larger NIJ effort and therefore was focused on technologies intended to enhance school safety.

For purposes of this report, technology is defined as any device or mechanism applied or installed in schools to prevent, mitigate, or deter criminal acts of violence in the school environment. Examples of safety-related technologies include, but are not limited to, surveillance cameras and communication systems, alarms, door locks and other entry control systems, weapons detection devices, emergency alert systems, protective glass, interior and exterior lighting systems, social media monitoring, and global positioning systems.

In discussing issues with school officials, it is at times difficult to separate school “violence” from broader discussion about safety and well-being of students, teachers, and staff. In interviews with

school officials and throughout the literature, discussion on school violence often is tied to topics such as bullying, cybercrime, substance abuse, traffic accidents, fire prevention, gangs, and trespass.

The authors restricted their exploration of technology to those that help school officials prevent or respond to acts of criminal violence. In that respect, the presence and use of firearms and other near-lethal weapons (e.g., pepper spray, Tasers) as violence prevention devices are not included. Neither are technologies intended to detect drugs. In addition, architectural considerations such as entrance redesign were excluded. Lastly, although planning and personnel are key components of any safety, security, and emergency program, they were not considered during the research.

Because of the role that social media plays in bullying, harassment, and bias, along with its use for general notifications (e.g., weather-related school closings), there is significant interest in social media monitoring. Moreover, it starts a conversation about where the boundaries of the school lie—within the physical property lines or into the community where the students live—and when the school’s responsibility to its students ends—at the end of the school day or around the clock.

The study team researched law and policy related to school security technology, but it did not focus on the ethical and moral issues associated with such tools. Even so, discussions with school officials about security technology frequently focused on concerns such as unnecessary and excessive purchases, the effect of technology in generating fear, lack of training on the use and assessment of technology, favoritism toward certain vendors, and the inability of schools to adequately maintain technology.

The study team’s work was limited by the following factors:

- There is no comprehensive source to locate data about technology deployment for school safety. Although the National Center for Education Statistics collects data on a limited number of security technologies, it is not comprehensive. There are few state databases on school security technology, and these are not aggregated.
- Schools are not required to report on the type of security technology in place, how it is funded, or how it is selected.
- Although anecdotal evidence is frequently cited, few schools and school systems monitor, assess, and report on the use and outcomes of security technology.
- Criminal acts of violence within schools are relatively rare events, which is fortunate for schools but makes the scientific and data-driven evaluation of the efficacy of specific technologies difficult to accurately assess.
- Much of the general information and research on the effectiveness of school security technology is vendor-driven.

In addition, although most school principals and other officials reported concern about day-to-day offenses (e.g., assault, bullying, theft), much of the focus of security technology has been on the prevention of and response to active shooters and mass casualty events. Focus on low-incidence, high-consequence events has been a priority since the Columbine High School shootings. According to individuals who provided input to this study, the continued focus on mass casualty events is driven by funding (Federal and state grants), school system mandate, media focus on such events, public sentiment, fear, and a genuine desire to foster effective prevention and response measures. The assumption made by many is that focus on prevention of and response to major events will positively impact prevention of and response to day-to-day and less serious violent offenses.

The lack of ongoing interaction among educators, scientists and engineers, law enforcement, and security personnel proved to be another limitation. Not many centers, institutes, professional associations, or other organizations focus primarily or routinely on bringing these professions together to address technology needs, issues, and successes. Ongoing connection across the professions responsible for design, application, response, and assessment of school security technology inhibits collective understanding, research, and further advancement of appropriate school-based security technology.

The information presented herein is current as of May 2016; moreover, technology, legislation, and literature all continue to evolve. Therefore, the lasting value of this study is to provide a way of thinking about implementing technology such as the planning process, the way technology is used in schools, benefits and concerns associated with a technology, cost considerations, and future considerations. None of the security technologies described herein are endorsed by the authors, school districts, National Criminal Justice Technology RT&E Center, or NIJ.

1.6 HOW TO USE THIS DOCUMENT

This report is intended to be used by a range of audiences, including school administrators, security directors, principals, and others. Although it may be read cover to cover, the authors developed their chapters as standalone documents that can be read sequentially or as needed by the reader. To receive maximum benefit, the chapters are intended to be used in conjunction with each other. For example, if one were interested in learning about a physical security information management system, or PSIM, the reader could turn to the chapter regarding software to learn about how the technology works. After learning that a PSIM integrates different kinds of technologies, the reader could turn to another technology-related chapter, such as alarms and sensors, to understand how they work. In addition, the reader could turn to the case studies to see if a jurisdiction had deployed a PSIM and learn about its benefits and why a district decided to implement it, additional information about how the technology is generally used, as well as acquisition considerations. Lastly, consulting the legal review chapter could provide a reader with information about legal implications of deploying such a system in their locale.

To help the reader find the appropriate information, the document contains the following chapters and information:

- Chapter 2, School Safety and Security Technology Implementation Planning, provides a perspective on the subject of risk management, one that is foundational to school safety technology planning, integration, and implementation. It focuses on how to assess the need for safety and security technologies and to develop a justification for their implementation.

There are eight technology category chapters spanning the technology categories reviewed. In each chapter, the technology is evaluated using the Federal Emergency Management Agency preparedness mission areas—prevention, protection, mitigation, response, and recovery—to offer a perspective on what makes the technology useful. In each chapter, specific technologies are itemized. Each technology is described, including its use in schools; benefits and concerns associated with the technology are discussed; cost considerations are listed; and a sample list of vendors is provided. Future considerations and other reading are also presented in some chapters.

- Chapter 3, Technology Review – Access Control, focuses on access control devices that prevent or otherwise control physical access to school property, people, and/or resources. These devices are some of the most widely used for school security and safety. Items like locks, fences, vehicle

barriers, turnstiles, bullet-resistant doors and window coverings, and lockdown devices are all discussed. In addition to the safety issues addressed by this report, these devices are also used to prevent theft and vandalism, to help ensure school visitors are more easily accounted for, and that specialized equipment and other items (e.g., cleaning chemicals, science laboratories) are safely secured.

- Chapter 4, Technology Review – Alarms and Sensors, focuses on alarms and sensors that operate autonomously to enable the early detection of intruders. Alarms also can be notification systems often triggered by a sensor. These devices are used inside or outside the school premises. Devices including motion sensors, open-door or open-window sensors, and duress alarms are discussed. The primary purpose of alarms and sensors is to speed up the notification and engagement of school and law enforcement officials in the event of a crime or emergency.
- Chapter 5, Technology Review – Communications, focuses on communications devices that are designed to facilitate or monitor the communication of personnel within the school or stakeholders outside the school such as first responders, administrators, or the surrounding community. This chapter reviews one-way communication devices, such as digital signs and public address systems, and two-way communication devices such as radios, telephones, and intercoms.
- Chapter 6, Technology Review – Lighting, focuses on security lighting. This is different from task lighting (i.e., the lights that enable work performance in a classroom, office, or laboratory), safety lighting (i.e., streetlights adjacent to a sidewalk that prevent trips and falls at night), and illuminated signs. Security lighting can be installed internally (indoor) and externally (outdoor) to the school building. Lighting can help deter crime and enable other technology like surveillance cameras.
- Chapter 7, Technology Review – Software Applications, focuses on software applications that are primarily used by school staff to analyze and combine electronic data and resources to improve school safety. Applications such as security planning tools, physical security information management systems, violence prediction software, visitor database checks, mental and public health information sharing, tip lines, and social media monitoring are discussed. The common role for all of these technologies is detection and mitigation of security risk.
- Chapter 8, Technology Review – Surveillance, focuses on surveillance devices that are intended to allow school personnel and responders to monitor and better understand situations as they arise. They enable an individual in a remote location to monitor students, school staff, school grounds, and school assets. Items such as surveillance cameras, gunshot-detection technology, radio frequency identification systems and global positioning systems location tracking, and unmanned aerial vehicles are discussed.
- Chapter 9, Technology Review – Weapons Detection, focuses on weapons detection systems that are designed to detect weapons concealed on persons or in their belongings. Usually they are intended to detect large or small quantities of metallic, organic, or explosive objects. Metal detectors and baggage scanners that detect weapons such as firearms, knives, and explosive devices are discussed.
- Chapter 10, Technology Review – Other Technology Systems, discusses a few school safety technology options that do not fit into the preceding categories but that are used in schools to improve safety. Items such as personal protection devices and privacy window films are discussed.

Following the chapters on specific types of technology, the report includes overviews of legal aspects of technology as applied to school safety, case studies describing how technologies have been implemented in a few U.S. schools, a literature review which may provide additional insight into existing information, and an overview of school safety strategies used outside the United States.

- Chapter 11, School District Case Studies, provides examples of school safety technologies deployed in four different school environments. It is a snapshot in time that provides context to the use of school safety technologies in real-world settings to gain an understanding of the current technology in use, its implementation, and considerations affecting implementation.
- Chapter 12, Legal Review, provides an overview of the statutory and regulatory law at the Federal and state levels that guide (by permitting or restricting) the use of technology in preventing or mitigating school violence. A search of media coverage of school safety and technology identified several local-level regulations as well as the nature of discourse regarding school safety and technology in major newspapers in the United States.
- Chapter 13, Literature Review, provides a perspective on school safety technology and fosters increased understanding of such technology as documented by officials in the fields of education, criminal justice, security, public health, and others. It draws on available academic literature and other published sources to assess the current understanding of the use of technology to prevent acts of criminal violence in Pre-K to grade 12 schools and advance and maintain a school's safety and security.
- Chapter 14, International School Safety Technology Review, provides perspective and comparison to the study of school security technology in the United States. This chapter focuses on the scope of school security methods and, particularly, technology-based approaches used worldwide. It draws on available academic literature and other published sources to describe what is known about the use of technology in a sampling of countries around the world.

1.7 STUDY TEAM

To meet the study tasks, the RT&E Center established a diverse team of scientists, engineers, researchers, and practitioners from law enforcement and education. The team was drawn primarily from three entities within JHU—the Applied Physics Laboratory; the School of Education, Division of Public Safety Leadership; and the Bloomberg School of Public Health, Center for Law and the Public's Health. In addition, subject matter authorities from education and law enforcement supported the effort.

Mr. Steven R. Taylor of the Applied Physics Laboratory served as Study Director. Other primary team members included the following:

Team Members	JHU Organization
Lauren Brush John Cristion Morgan Gaither Alexander Ihde Subramaniam Kandaswamy William McDaniel Kelly O'Brien Phillip Pratzner Patrick Shilts	Applied Physics Laboratory
Anna Davis Stephen Teret Julia Wolfson	Bloomberg School of Public Health, Center for Law and the Public's Health
Sheldon Greenberg	School of Education, Division of Public Safety Leadership

Chapter 2. SCHOOL SAFETY AND SECURITY TECHNOLOGY IMPLEMENTATION PLANNING

Steven R. Taylor, MPA; Phillip R. Pratzner, MS; and William R. McDaniel, PhD

At the end of the day, the goals are simple: safety and security.

—The Honorable Jodi Rell, former Governor of Connecticut

There is no such thing as perfect security, only varying levels of insecurity.

—Salman Rushdie

2.1 INTRODUCTION

Incidents of extreme violence like those at Columbine High School in 1999 and Sandy Hook Elementary School in 2012 garnered a tremendous amount of attention and resulted in increasing public and political scrutiny, leading to a call to assess ways to secure our classrooms and campuses more effectively. In many instances, this sparked a rapid increase in the use of technology to ensure the safety and security of pre-Kindergarten (Pre-K), elementary, middle, and high schools. In an article for National Public Radio, Cathy Paine, chair of the National Association of School Psychologists Emergency Assistance Team, notes that the chance that “an armed intruder will come in [is] 1 in 2.5 million.” She went on to suggest that schools should have comprehensive safety programs that consider both the worst case and the more likely crises. She indicated that rather than focusing on protection against a shooter, a better approach would be to balance efforts to ensure physical safety of the campus, such as perimeter fencing and controlled building access, with efforts to address “psychological safety” such as bullying (Reference 145).

The first question one should ask when thinking about school safety and security technology is: What problem am I trying to solve? There are myriad issues that schools confront—some daily, some never. These range from smoking in the bathroom to graffiti on the wall to theft of school supplies to bullying in the cafeteria to intruders to kidnapping or a school shooting. Each of these incidents may require different solutions that may or may not include technology. This makes it essential for the school or district to research the link between the problems and proposed mitigation actions. Security technology cannot solve all school security problems; technological solutions should be integrated into broader prevention and intervention measures, ranging from practicing crisis response drills to building a positive school climate (Reference 302).

This chapter provides background on the general state of literature regarding technology planning and the techniques used to support and justify technology deployment. Next, planning processes and planning teams and their applicability to the choice of security technology are discussed. Although comprehensive risk management guidance is not provided, an overview is provided of some common techniques and components of that process. In addition, a process for setting security objectives and security technology choices is described. This chapter concludes with a brief description of the need to iterate on decisions to deploy technology.

While there is a plethora of technology available to schools, as Ken Trump notes in a National Public Radio article, “There is a security product for every possible need that your budget will buy. The question is, is that the best use of limited resources?” (Reference 145) This intent of this chapter is to

provide background that will guide the school practitioner to best match technology capability with the problem.

2.2 BACKGROUND

Many public schools have become high-security environments (Reference 39). A study of security technology in U.S. schools based on information from Common Core of Data (90,000 schools) found that 98.6% of schools reported using security technology (Reference 75). School safety and security technology spans a broad range of items—from low-technology devices such as lights, doors, locks, and door pins, to, at the other end of the spectrum, metal detectors, surveillance cameras with video analytics, social media tracking software, infrared detection, and sophisticated school-to-police communication systems. Many of the security solutions recently deployed in schools rely on technologies developed by military and security industry engineers beginning in the 1940s for police and national security purposes during the Cold War. In schools, fear of violence and of legal liability are rationales that school district administrators use to expend resources on security technology. The National Alliance for Safe Schools notes that schools have become a major and growing market for the security industry (Reference 56).

There is a large volume of general literature on risk assessment and planning tools for schools. Numerous articles call for schools to conduct risk assessments, and a large number of online sites offer risk assessment toolkits. One general guide to such assessments is *A Guide to School Vulnerability Assessments: Key Principles for Safe Schools*, published by the U.S. Department of Education (DoED) Office of Safe and Drug-Free Schools in 2008 (Reference 356).

The Guide states the following:

Crises affect schools across the country every day. While natural hazards such as tornadoes, floods, hurricanes, and earthquakes may be thought of more commonly as emergencies, schools are also at risk from other hazards such as school violence, infectious disease, and terrorist threats. Through the vulnerability assessment process, schools can take steps to prevent, mitigate, and lessen the potential impact of these risks. ... Vulnerability assessment is the ongoing process for identifying and prioritizing risks to the individual schools and school districts. It also includes designing a system of accountability with measurable activities and timelines to address risks.

The scholarly literature is extensive in addressing the need for risk assessment in schools and commonly cites the components of risk assessment tools and processes; however, few sources evaluate these tools and processes. Major organizations, Federal agencies, and state school systems provide risk assessment information, guidelines, and tools. While some tools primarily target assessing high-risk and potentially violent behavior, almost all give attention to facilities and technology. The following is a small sample of the information available:

- Eastern Kentucky University – *School Critical Incident and Risk Assessment*¹
- Florida DoED – *Safe Schools Design Guidelines: Strategies to Enhance Security and Reduce Violence*²
- National Institute of Standards and Technology – *Risk Management Framework*³

¹ <http://jsc.eku.edu/SCIP>

² http://www.fldoe.org/edfacil/safe_schools.asp

³ <http://csrc.nist.gov/groups/SMA/fisma/framework.html>

- New Jersey DoED – *School Safety and Security Plans: Minimum Requirements*⁴
- North Carolina Department of Public Instruction – *Safe Schools Facilities Planner*⁵
- Texas School Safety Center – *Campus Safety and Security Audit Toolkit*⁶
- Virginia DoED – *School Safety Audit Protocol*⁷

Decisions about whether to invest in school security technology for a school or school district are complex and must take into account a variety of logistical, economic, and political factors. In some cases, minor improvements are required to address safety concerns. As Schneider (Reference 302) notes, security technologies, such as those referenced in Chapter 3 to Chapter 10 in this report, provide many tools schools can point to as measures they have taken to enhance student, visitor, and staff safety. Although security measures are often crisis-driven, schools should consider the following items before acquiring and deploying technology:

- A positive school climate is paramount for learning; technology should not create a prison-like atmosphere or generate additional fears.
- Technology cannot compensate for inherent building design weaknesses.
- Without training, technology can prove ineffective.
- Without the appropriate culture, technology can be circumvented.
- Technology may evolve rapidly (and so does the software that may accompany it); consideration must be given to replacement, maintenance, and repair costs.
- Long-term support for the technology is a key factor; support from unproven vendors or distributors is unknown.
- Technology selection should focus on addressing a specified problem.

A comprehensive evaluation should be conducted before choosing a technology “solution.” The evaluation could draw on a number of approaches, including user surveys and safety audits, risk management, analysis of alternatives, and other tools. Districts and schools with chronic violence or small budgets should not take the same approach as those where violence is rare or budgets are large. Ultimately, Schneider states, schools should bring the technology evaluation “back to the original problem being addressed, and see if the technology is a good match.” (Reference 299)

When considering which school safety and security technology to select, it is important to use the tools available to justify and document the decision. Assessments such as needs assessments, threat assessments, risk analysis, safety and security audits, hazards assessments, and facilities assessments may have some utility. Analysis of alternatives, cost-benefit analysis, and analysis of strengths and weaknesses may play a role in making a reasoned decision.

2.3 THE PLANNING PROCESS

“In the past, schools have rarely understood the need or had the time or resources to consider their security plans from a systems perspective—looking at the big picture of what they are trying to achieve in order to arrive at the optimal security strategy. A school’s security staff must understand what it is trying to protect (people and/or high-value assets), who it is trying to protect against (the threats), and the general environment and constraints that it must work within—the characterization of the facility.

⁴ <http://www.nj.gov/education/schools/security/req/req.pdf>

⁵ www.schoolclearinghouse.org/pubs/safe2013.pdf

⁶ <https://txssc.txstate.edu/tools/emergency-management-toolkit/role-of-districts/audits/k12/conducting-audits>

⁷ http://www.doe.virginia.gov/support/safety_crisis_management/school_safety/audits/sch_safety_audit_protocol.pdf

This understanding will allow a school to define its greatest and/or most likely risks so that its security strategy consciously addresses those risks. This strategy will likely include some combination of technologies, personnel, and procedures that do the best possible job of solving the school's problems within its financial, logistical, and political constraints. Why is this careful identification of risk important? Because few facilities, especially schools, can afford a security program that protects against all possible incidents." (Reference 139)

The literature review (Chapter 13) revealed that the term "school safety" is very broad, incorporating everything from crosswalk safety to protection from an active shooter. Although "security" as a word has a similar meaning to "safety" and there is minimal difference between feeling secure and feeling safe, the two terms do have different meanings. Safety is used when the threat is an unwanted side effect of something else wanted. Safety thus is associated with incidents and accidents. Security is protection against malicious acts such as sabotage or terrorism. There is a grey area where the distinction between security and safety, between accident and criminal act, is difficult to draw (Reference 7).

However, the focus for the report and this particular chapter is on technology that mitigates acts of criminal violence. Practically speaking, this narrows the definition from all potential threats to those more aligned with a common definition of security—the state of being protected or safe from criminal violence.⁸ This includes incidents such as a group of delinquent students whose intent is to destroy and deface school property, a physically aggressive bully, or an active shooter.⁹ However, this definition does not include situations such as a fire in the kitchen, an accident at a school crossing, or the response to a severe winter snowstorm. Unfortunately, there is no "one size fits all" technology that can prevent any and all bad things from happening in a school. Elements of security should be reviewed not only for their ability to reduce potential loss, but also their ability to reduce the fear of criminal violence (Reference 186).

As stated by Summers et al. (Reference 333), "A big risk is not addressed by a big list: it is addressed with the right list of independent protection layers." When considering the acquisition of a technology, it is important to understand the problem that needs to be solved and match the capability of the technology to the problem or maximize the number of problems that a technology addresses. This requires those responsible for implementing security technologies to use a process for assessing school security, particularly about justifying the acquisition of technology to counter acts across the spectrum of criminal violence.

The literature describing methods for conducting a planning process is extensive. Generally, however, a reasoned justification identifying the need and the rationale for selecting a particular technology is warranted. This requires a repeatable process to evaluate security technology requirements, which is frequently lacking (Reference 2). Moreover, technology decisions may be determined with incomplete information or information that is influenced more by political or reactionary consideration than by local conditions (Reference 156).

⁸ This definition is based on Merriam-Webster's definition of security. However, "criminal violence" is added for purposes of this review.

⁹ The state of Florida lists 25 incidents that require reporting. Florida Department of Education, 2013–14 Automated Student Information System, *Appendix P: Definitions for Incident Reporting*. <http://fldoe.org/core/fileparse.php/7670/urlt/0101000-appendp.xls> Retrieved 26 October 2015.

Atlas (Reference 17) provides general principles for safe and secure school design. These principles include the following:

- Define threats and vulnerabilities to attack and loss.
- Define assets that are worthy of being protected.
- Characterize the environment and balance the needs to the threats.
- Determine acceptability of proposed security technology and practices.
- Calculate the affordability of technology and features.

The engineering design process (EDP) is another useful construct for choosing a security technology. At its core, EDP defines the problem by seeking responses to three questions (Reference 322):

- What is the problem or need?
- Who has the problem or need?
- Why is the problem important to solve?

The U.S. DoED (Reference 355) recommends a planning process for developing school emergency operations plans. This process can easily be adapted to fit the planning needs of security technology implementation.

- **Form a Collaborative Planning Team.** Include individuals representing the schools, school district, and stakeholders with input to security threats in the planning team.
- **Understand the Situation.** Identify threats, hazards, risks, and vulnerabilities in and around the school(s) or district.
- **Determine Goals and Objectives.** Determine which threats and hazards will be addressed.
- **Identify Courses of Action:** Generate, compare, and select possible solutions based on the goals and objectives.
- **Plan Preparation, Review, and Approval.** Develop procedures and incorporate technology into existing plans.
- **Technology Implementation and Maintenance.** Train, exercise, assess, and maintain technology and associated plans.
- **Iterate.** Repeat the process periodically; for instance; during budget cycles or at the end of a life cycle.

These examples represent a small sample of the types of resources available to assist with selecting technology. The information technology and systems engineering fields are replete with guidance materials, much of which looks similar or has some variation on the preceding themes. Some are more prescriptive, whereas others provide a simple framework. Neighboring school districts, national organizations, or state and Federal agencies may have guidance and technical assistance available for selecting school safety and security technology. In all cases, however, school or district acquisition policies and processes should be followed when considering the purchase and deployment of security technology.

2.4 PLANNING TEAMS

A collaborative planning effort, including a strong planning team, is an effective way to gain acceptance and buy-in. Many schools have a safety and security committee or an action team. Leveraging such a team can provide a “leg up.” However, research is required to confirm or dispute suspected safety and

security problems as well as resulting improvements (Reference 242). Beard and Brooks (Reference 26) believe a consensus approach to risk assessment can provide valid outcomes.

Developing a planning team that includes individuals who are knowledgeable about different areas of the district, school, and surrounding community is necessary for optimal decision-making. Many business and government resources describe how to assemble effective planning teams. For example, DoED and the Federal Emergency Management Agency (FEMA) recommend that including members from the district administration, the school security community, technology services, teachers, school counselors, emergency response personnel, community members, parent teacher associations, school architects, and other stakeholders may be valuable, depending on the school district and the issues under consideration (References 111 and 355).

A planning team fulfills several important roles—identifying individuals knowledgeable about school hazards, threats, vulnerabilities, risks, and security technology, and ensuring a variety of perspectives are represented. The team can consider new or upgraded safety technologies, implications to the school environment, and ongoing material and staffing requirements; act as a liaison to provide continuity across safety and technology planning; and ensure better integration with existing equipment and appropriate upkeep and replacement of technologies. Lastly, team members can help to address any policy issues that may arise from their communities, highlighting possible roadblocks for technology implementation. One best practice identified is documenting the planning process and identifying planning team members and stakeholders to provide a permanent record of who was involved and how decisions were made (Reference 111).

The Connecticut School Safety Standards recommend that a School Safety Design Committee be established for each school construction project. This committee's role is to review and assess the safety and security needs of the school facility and make recommendations about safety and security features (Reference 329). In addition, the New Jersey School Security Task Force highlighted a best practice of convening a district and school level planning team in its task force report (Reference 306). Lastly, the Sandy Hook Advisory Commission recommends (Reference 297): "Each community or school district should have a small standing committee or commission, comprised of individuals representing the school community, law enforcement, fire, [emergency medical services] and public health, whose responsibility is to ensure that the [safe school and design operations] standards and strategies are actually implemented in their community."

Decisions on safety and security technologies have a broad impact on the school environment. Prior to acquiring safety and security technology, recommended practices suggest formation of a collaborative, well-documented planning team.

2.5 UNDERSTAND THE SITUATION

Implementation of technology in schools is intended to prevent or mitigate acts of criminal violence. By implementing a security technology, school officials can reduce their exposure to risk or the possibility that something harmful is going to happen in their district, building, or location.

The ultimate objective of the risk assessment process is to find the most effective mitigation measures to achieve a desired level of protection against a wide range of threats. Generally, a district or school needs to understand the likelihood that a specific threat or hazard will occur and the effects it likely will have. These effects include the severity of the impact, the amount of time the school will have to warn students and staff about the threat or hazard, and how long an incident may last. In addition,

characteristics of the school (e.g., structure, equipment, infrastructure, grounds, and/or surrounding area) that could make it more susceptible to the identified threats and hazards are important to catalog (Reference 355). Figure 2-1, derived from Department of Homeland Security (DHS) literature (Reference 60), generalizes this approach to the following:

- Consequence assessment and threat and hazard assessment contribute to a vulnerability assessment,
- A vulnerability assessment contributes to a risk assessment.
- A risk assessment leads to identifying mitigation options,
- Mitigation options inform a decision.

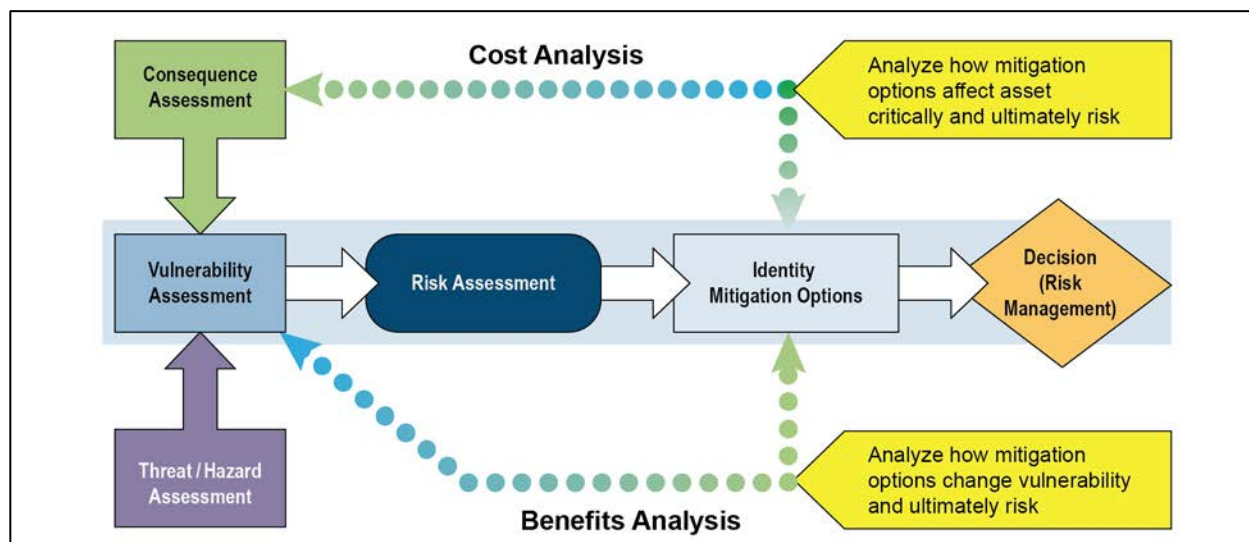


Figure 2-1 Risk Assessment Process Model

The literature, mostly not school-specific, contains many resources that describe how to systematically collect and analyze this type of information, allowing school representatives to make informed decisions about security technology acquisition and deployment.

2.5.1 IDENTIFY ASSETS

By enumerating the assets a school must protect, the basis is laid for conducting a thorough risk assessment. Much of the literature agrees that the first step in a risk assessment process involves identifying who or what needs protecting. This can take the form of listing, enumerating, and categorizing the assets that the school should protect (Reference 11). Assets can be anything that possesses a value to the school or district, including students, staff, or visitors, and may be information, property, or equipment and supplies (Reference 9). DHS categorizes assets as tangible (e.g., students, faculty, staff, school buildings, facilities, equipment, activities, operations, information) or intangible (e.g., processes or school's reputation). Furthermore, people are a school's most critical asset (Reference 60).

Documenting responses to the following set of questions, according to Atlas (Reference 17), is a good way of cataloging assets that require security protection.

- What are the assets (persons, places, information, property) that require security protection?
- Who are the users (visitors, staff)?

- What can the users do in the building (tasks, recreation)?
- Why are the particular users there (official business, guests)?
- When do the users arrive and leave (time, shift, patterns)?
- Where can users enter the building?
- How can the users get there (access methods, pedestrian and vehicle circulation)?
- What information (about students, staff, visitors, etc.) is collected and stored?
- Where is essential equipment and supplies stored?

Green (Reference 139) also discusses a school's assets and agrees that protection of the students and staff is most important. In addition, she notes that measures taken to protect a school's assets are usually driven by defined threats and that schools cannot afford to protect all their assets to the same degree.

2.5.2 IDENTIFY THREATS

After identifying assets, the literature asserts that it is important to identify threats. As Lincke (Reference 205) notes: "a 'threat' is only a concept; the word 'threat' does not imply that [a] problematic event has actually occurred." To identify threats, investigate incidents that have occurred at the school or in the district and review data on crime statistics in and around the school. It is important to distinguish threats in the general environment from threats in the school environment. For instance, burglary may be a common crime in the school district, but the school, as a hard target, may be at a low risk for this threat. In addition, the data should be reviewed for trends to determine whether a particular threat is on the rise or decline.

Experts such as local law enforcement or emergency management (depending on how broadly the term "threat" is defined) or state school safety resources or other Federal DoED or national associations are good sources of threat information. Students themselves may be a good source of information about school crime and problem areas; likewise, school resource officers, teachers, and school administrators, facility managers, and neighbors should all be consulted (Reference 17).

Threats to a school generally can be classified as external (e.g., outside influences and persons) or internal (e.g., students, faculty, staff, workplace violence). In Connecticut, school construction grant applications must be accompanied by a risk assessment of the site. An "all hazards" approach is required in assessing critical assets, identifying vulnerabilities to natural or manmade hazards, and determining effective mitigation measures that provide a level of protection (Reference 329). FEMA routinely categorizes and publishes threats or hazards (Table 2-1 from Reference 362).

Lincke (Reference 205) categorizes hazards similarly; however, she expands the human-caused hazards to include fraud, espionage, hacking, identity theft, malicious code, social engineering, vandalism, terrorists, hacktivists, disgruntled employee, or student violent attack. Wayland (Reference 380) adds active shooter, bombs and bomb threats, computer crimes, explosions, fire, gang activity, homicide, hostage, kidnapping, illegal drug possession or sales, pilferage, records manipulation, sexual harassment, theft and burglary, vandalism, and violent or uncooperative visitors. The Florida Department of Education has a list of "reportable incidents;" other states may have similar requirements. These incidents include alcohol, arson, battery, breaking and entering, bullying, disruption on campus, drug sale or distribution, drug use, fighting, harassment, homicide, kidnapping, robbery, larceny, sexual battery, sexual harassment, tobacco, threat or intimidation, trespassing, vandalism, and weapons possession (Reference 120).

Table 2-1 FEMA-defined Threats

Natural Hazards	Technological Hazards	Human-caused Hazards
Avalanche	Airplane crash	Civil disturbance
Disease outbreak	Dam or levee failure	Cyber events
Drought	Hazardous material release	Terrorist acts
Earthquake	Power failure	Sabotage
Epidemic	Radiological release	School violence
Flood	Train derailment	
Hurricane	Urban conflagration	
Landslide		
Tornado		
Tsunami		
Volcanic eruption		
Wildfire		
Winter storm		

Scenarios based on identified risks provide a context for assessing their effects and potential impacts. By enabling the team to consider activities before, during, and after an incident, analysis of the scenario can indicate times and places where a potential negative event could be disrupted and the risk reduced.

There are many lists of threats from which to gather information in the literature. However, it is important to consider exclusion or omission because there is always a potential for new and unexpected risks. Also, a list may give the impression that hazards are independent of one another, when in fact they are often related. The list should be vetted with the planning team and stakeholders and reviewed periodically.

2.5.3 ESTABLISH LIKELIHOOD

Although it can be difficult to accurately gauge the likelihood of a threat occurring, it is an important component of the risk assessment process. Estimating the probability or likelihood the threat will occur is mentioned frequently in the literature. One method is to gather historical data about threats in the school environment and evaluate trends. Lincke and Wayland suggest that despite the challenge in finding appropriate data, it is important to consider the likelihood of an event occurring due to a threat; past experience, analysis, or a best guess are all accepted practices for obtaining the data. Selecting good statistics to derive an exact probability is a challenge at best and impossible at worst; past experience or a group-based best guess may be the best that can be accomplished (Reference 205).

Some writers suggest it is not necessary to conduct exhaustive research and that simple, subjective historical data based on local crime rates and societal factors is sufficient. Wayland describes a simple method wherein a number between 1 and 10 (1 being the incident is improbable and 10 being the event could occur frequently) is assigned to each threat; to reduce its subjectivity, the likelihood score is reviewed and coordinated between local law enforcement and internal stakeholders (Reference 380). Similarly, Smith and Brooks provide a one-to-six likelihood scale (Table 2-2 from Reference 322).

Table 2-2 Likelihood Scale

Scale	Rank	Descriptor
Certain	1	The event will be realized
Very high	2	Highly probable
High	3	Probable
Medium	4	Moderately probable
Low	5	Improbable
Unknown	6	Likelihood of event unknown

When conducting likelihood analysis, the following factors are noted as being important (Reference 17):

- Does the school building or its occupant invite potential hostility?
- Is it conspicuous or does it have symbolic value?
- Does the building appear vulnerable?
- Have school buildings been targets in the past?

The Florida Safe Schools Project Update found that in 2002–2003 there were fewer fights and disorder problems at elementary and high schools compared to middle schools. In addition, survey participants reported that fighting, disorderly conduct, and vandalism are the three most common crimes on their campuses (Reference 190). Recent data report that, overall, theft generally is the most common non-violent crime on school campuses (Reference 17).

2.5.4 IDENTIFY VULNERABILITIES

Understanding the vulnerabilities of specific schools and the types of threats posed at their locations permits development of effective countermeasures. Vulnerabilities are weaknesses that, when exploited, can harm school assets. An example of a vulnerability might be an open door, which increases the possibility of an unauthorized and dangerous person entering the school building. It is important to estimate the degree of vulnerability that exists for each asset and threat pair (Reference 9).

Risk assessment literature contains many examples of vulnerabilities. A subsection of risk mitigation, called crime prevention through environmental design (CPTED), applies natural access control, surveillance, territoriality boundary definition, management, and maintenance strategies to reduce external threats and vulnerabilities. CPTED includes policy and procedure strategies and management techniques to reduce internal threats.

As a way of scoping asset vulnerability, a “defense-in-depth” concept may be useful. Originally a military strategy but now integral to professionals from various non-military fields and disciplines including information security (Reference 250), fire prevention (Reference 245), and nuclear safety, defense-in-depth presents a series of layers that deter and delay an intrusion until such time as an appropriate response is mounted (Reference 322). For the purposes of this chapter, these layers include cyberspace, outside the perimeter of the school grounds, within the school grounds, within the school building, and the subdivisions inside the building. These layers can be viewed as concentric rings with the school at the center temporally and geographically (Figure 2-2).

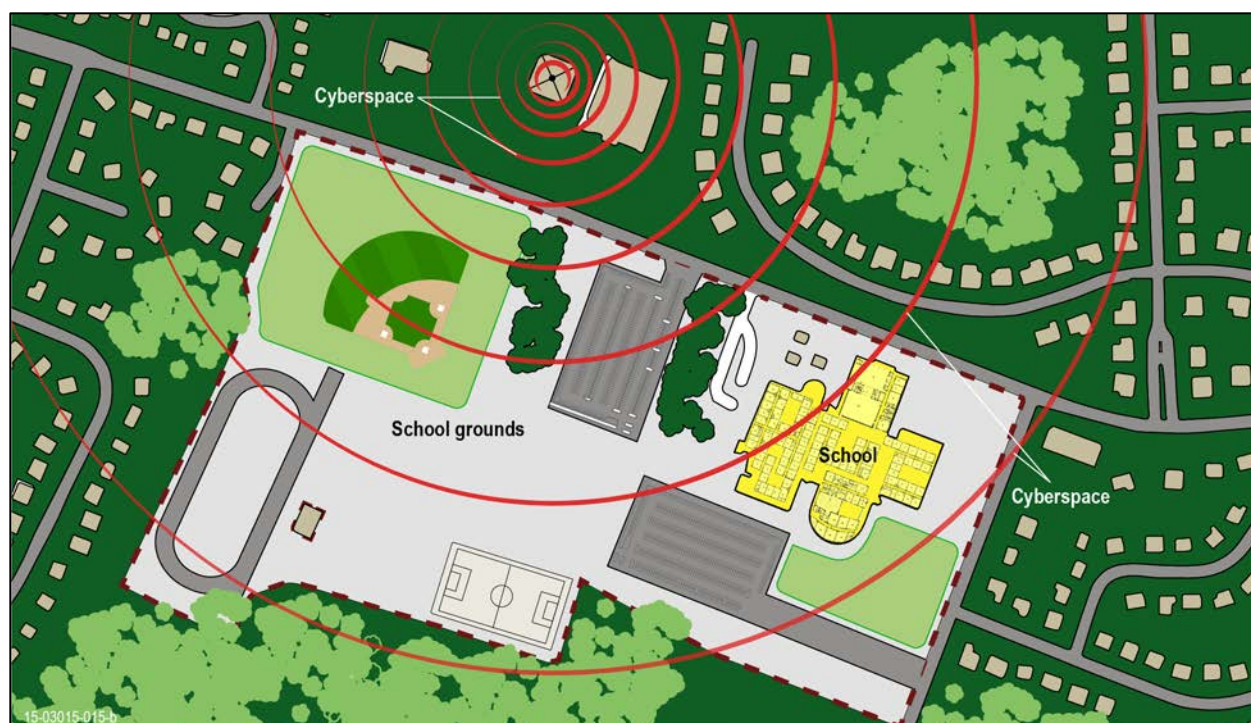


Figure 2-2 School Defense-in-Depth Layers

Research conducted for the Florida Safe Schools Guidelines identified parking lots, off-ground adjacent buildings, locker rooms, and restrooms as the top four places for crime; rooftops of covered walkways, building rooftops, lobby and reception areas, and main entrances had the lowest reported criminal activity. Incidents varied by location (e.g., vandalism or trespassing in parking lots or larceny, theft, and fighting in locker rooms) (Reference 17)

Another viewpoint for an individual school is:

- Geographic
 - Community boundary
 - Boundaries of feeder schools (e.g., a middle school may receive rising 5th grade students from an elementary school and supply rising 8th grade students to a high school)
 - School's attendance boundary (e.g., bus routes)
 - School ground's physical boundary
 - School building, i.e., classrooms, hallways, offices, and assembly spaces (e.g., cafeteria, auditorium, library, gymnasium)
- Cyber: Where the students, staff, visitors, and others who have reason to be in a school "live" virtually

Connecticut (Reference 329) and Atlas (Reference 17) are two of numerous sources that provide lists of potential vulnerabilities. Some considerations include the school site perimeter, parking areas, pedestrian routes, playgrounds, athletic and multipurpose fields, interior gathering locations like classrooms, cafeterias, or gymnasiums, roofs, and critical infrastructure and utilities. In addition, it is

important to consider *when* people (e.g., staff, students, and visitors) use the location and *why* they are there (e.g., attend class or after-school function).

2.5.5 IDENTIFY CONSEQUENCES

The analysis of potential consequences associated with a threat is one component of the risk assessment that can assist with selecting appropriate countermeasures. Estimating the potential degree of impact, or consequence, of the threat to an asset is important when prioritizing risk. Some authors writing about risk, though not all, add impact as a factor in the risk equation. This requires an estimate of the value of the asset being threatened (Reference 11).

The literature discusses the calculation of consequences and the significant variation that can occur. In many cases, the “worst case consequence” or “worst credible consequence” is used. Direct experience with either of these cases can provide a strong positive or negative bias. These qualitative biases may be great enough to push the impact estimate to a more or less conservative result than is appropriate (Reference 333). As with likelihood, a consensus approach is suggested by Beard and Brooks. They also note that such measurements of likelihood and consequence only provide an estimation of risk and caution that the relationship may not be absolute or linear (Table 2-3, from Reference 322).

Table 2-3 Consequence Scale

Scale	Descriptor
Catastrophic	Organization will cease to function if harm is realized
Very high	Major impact on organization’s ability to function and may lead to a prolonged period of non-functioning
High	Significant effect on organization’s operations and activities
Medium	Impact on organization’s ability to function, but recoverable with little effort
Low	Impact to organization covered by usual allowances
Unknown	Consequence of harm being realized is unknown

2.5.6 ASSESS RISK

By completing a risk assessment, schools can develop a data-driven justification for matching the problem to a potential solution or solutions. The objective of assessing risk is to gather, analyze, and communicate information about threats, likelihood, assets, vulnerabilities, and consequences in a way that allows a school official to decide what actions to take. Actions such as acquiring security technology are intended to create a level of protection that reduces the vulnerabilities to threats and their potential consequences, thereby reducing risk to an acceptable level. The literature on assessing risk generally is extensive, whereas that specific to schools is limited.

Increased interest in, and acquisition of, security technology often results in increased costs. There is typically reluctance to design for all of the security features that might seem prudent or reasonable. The challenge for most security professionals is that the terms used in the risk assessment process have become muddled and interchanged over recent years, so the subtleties of the differences have become lost. The Interagency Security Committee and FEMA models represent the most current view of risk in the risk community (Reference 17).

Risk can be generally thought of as a function of the values of threat, consequence, and vulnerability (Reference 361). FEMA and homeland security literature describes risk in one of two ways: (1) as a multiplicative combination of threat, vulnerability, and consequence (mathematically: $R=T*V*C$) or (2) as some other function of threat, vulnerability, and consequence (mathematically: $R= f(T,V,C)$). Other disciplines (e.g., insurance or environmental protection) may have different definitions of risk. As Young notes, there are other considerations, such as likelihood or the relative importance of each component of the equation, that suggest these equations should not necessarily be taken literally (Reference 390).

The literature suggests a number of methods for assembling the data for the risk analysis. A simple list, with a risk score assigned to each asset, can be created. Lincke uses a simple plot with likelihood and consequence—or impact—to visualize the risk analysis (Figure 2-3, from Reference 205). DoED creates a table based on multiple factors such as likelihood, consequence, and warning (Figure 2-4) (Reference 355). Chapter 7 of this report also includes a discussion on risk assessment tools that facilitate risk assessment.

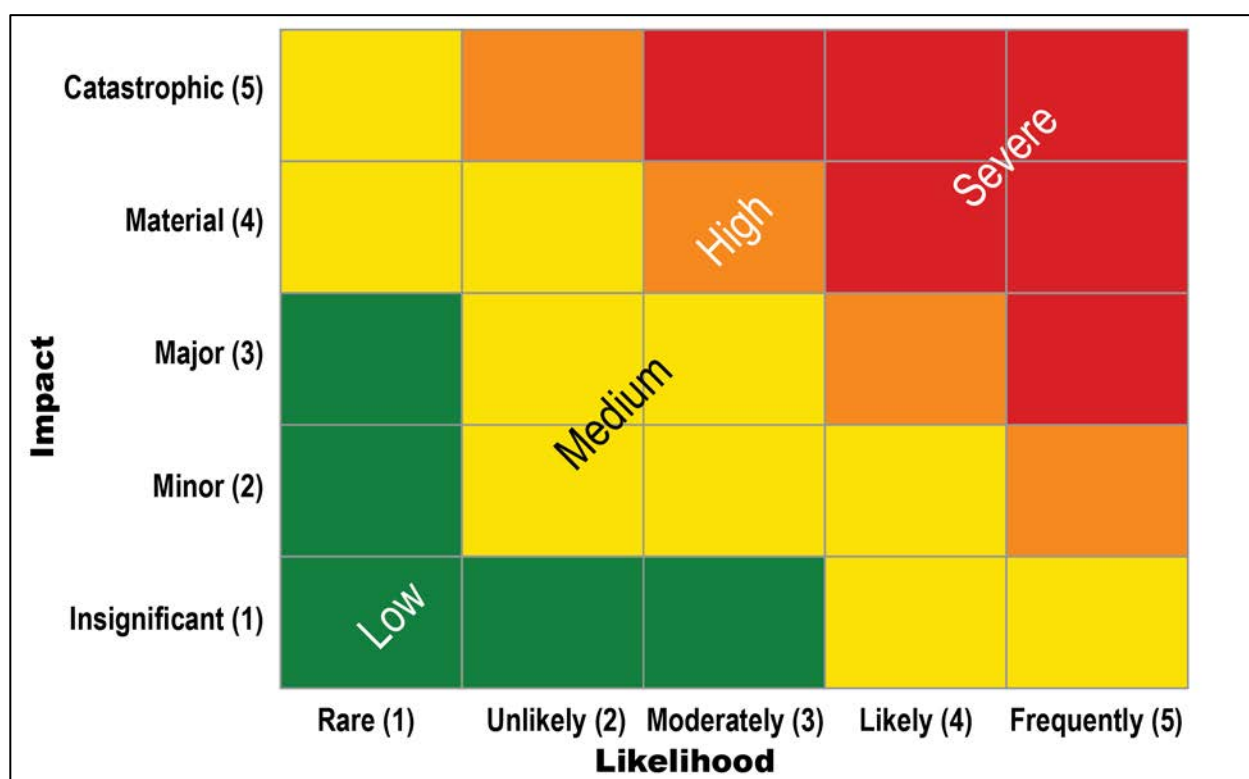


Figure 2-3 Semi-quantitative Risk Assessment

Threat	Score	Likelihood	Consequence	Warning	Duration
Active Shooter					
1	Unlikely	Negligible	24+ hours	< 3 hours	
2	Possible	Limited	12–24 hours	3–6 hours	
3	Likely	Critical	6–12 hours	6–12 hours	
4	Highly likely	Catastrophic	Minimal	12+ hours	
Assign a score for the four categories and write them below, then add the column scores to get the total risk value.					
Total	1	4	4	1	10
Risk Key: LOW ≤ 5; <u>MEDIUM 6-11</u> ; HIGH >12					

Figure 2-4 Sample Risk Assessment Worksheet

A risk assessment is useful in determining the potential impacts of threats and hazards to the assets in an individual school or across a district. The risk assessment can provide the foundation and justification for identifying and prioritizing actions, including the acquisition of security technology. No matter the method used, the end result should be a prioritized list of security risks for the school. School officials should vet their assessed risks and assigned prioritization against the environmental bounds imposed by local and school mandates, political and parental concerns, and, lastly, police and local fire department professional judgment and advice. These considerations may result in a reprioritized list, but one with buy-in from key constituencies.

2.6 DETERMINE GOALS AND OBJECTIVES AND SELECT COURSES OF ACTION

Once data have been assembled, the following question must be answered: What is it that the school system is trying to accomplish? Although not a simple either/or proposition, frequently choosing what to do in response to the assembled data may be a choice between addressing the greatest risk or addressing the most frequent problems, but often the decision made does a little of both. The literature discusses two approaches, minimizing likelihood and minimizing impact (Reference 205), but these are not the only considerations. Schools face political concerns, parental concerns, or community norms as well as legal considerations that do not support the idea of “letting the data guide them.” (Reference 244) Moreover, it is important to understand the organizational culture of a school and community to gain acceptance with decision-makers on implementing security measures (Reference 322).

As Young notes (Reference 390), in the absence of security incident statistics or a proper laboratory to conduct controlled experiments, the effectiveness of security controls cannot be rigorously tested. Often, solutions are implemented without really understanding their effect on the security risk profile. By identifying goals and objectives, a strategy that prioritizes the set of risk-mitigation measures proportionate to the identified threats can be developed.

Traditional goals and objectives of security solutions to each area of vulnerability include detect, delay, and respond. Green expanded this model in a school environment to deter, detect, delay, respond, and investigate (Reference 139). New Jersey took a similar approach by recommending that security measures be applied in a layered manner, starting at the perimeter, at the exterior of the building, and then proceeding to the interior. They also noted that security measures “provide a deterrent [and that] visible security measures offer a sense of security to students, staff and guardians, which is often as important as actual security.” (Reference 306)

Smith and Brooks (Reference 322) recommend a defense-in-depth approach with the following layers: *deterrence, detection, delay, response, and recovery*:

- **Deterrence** is achieved when security measures are sufficiently strong that breaching of a barrier is perceived as too difficult to defeat. It is a psychological effect that may be achieved with signage, lighting, defined boundaries, and response personnel. The efficacy of deterrence is difficult to measure.
- **Detection** is achieved when security measures detect a threat from a variety of sensors including personnel, electronic detection, or closed-circuit television and activates an alarm. Early detection of an intruder facilitates apprehension and deterrence.
- **Delay** is achieved through the use of physical barriers such as fences, walls, doors, and locks, all of which must be successively defeated to reach the assets of a school.
- **Response** is an action taken at the location of the detection that either apprehends or drives away an intruder.
- **Recovery** is the resilience of a school or district to rebound from an incident or crisis, achieved through appropriate planning.

DHS and DoED, informed by Presidential Policy Directive 8, are organized around five mission areas—prevention, protection, mitigation, response, and recovery. With regard to security planning, these mission areas are arranged along a continuum from proactive to reactive in terms of timing—before, during, and after an incident. The seriousness of the risk or threat will determine how early in the timeline it is appropriate to intervene. For instance, a scenario wherein the individual is intent upon harming many students and teachers may require early intervention (e.g., prevention), whereas an individual who is defacing school property may be disciplined, as appropriate, after the incident (e.g., recovery). Incorporating the five mission areas into school safety planning will align vocabulary, processes, and approaches with first responders in the community (Reference 355). The portion of the preparedness cycle upon which a school focuses drives the course of action. Each technology chapter in this report aligns its content across these five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident

from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.

- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

After defining security objectives and goals, it is important to begin to determine the range of technical and non-technical solutions that can satisfy these objectives; options include acquiring security technology, equipping or adding security personnel, developing security or response plans, or providing additional training. The intent of security planning is to identify safety and security improvements a school could pursue and how they may be pursued (Reference 242). Some of the literature suggests an assessment that results in a set of recommended countermeasures to specific threats that is priced, prioritized, and presented to decision makers for selection (References 9 and 17).

Although school safety technology is the focus of this report, it is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district. In the information technology realm, implementing measures to mitigate risks are referred to as controls. Generally, controls are divided into three categories: physical, logical, and administrative (Reference 11).

- **Physical controls** protect the physical environment. They include items such as fences, gates, locks, bollards, guards, and cameras.
- **Logical controls** protect the environment with technical solutions like sensors and intrusion detection.
- **Administrative controls** set out the rules such as laws, policies, procedures, guidelines, plans and training.

Alternatively, when examined from a DHS or DoED mission area perspective, the range of options can appear different (Reference 357).

- Prevention and mitigation addresses what schools and districts can do to reduce or eliminate risk to life and property. For example,
 - Establish access control *procedures* and provide identification cards and access control *technology*.
- Preparedness focuses on the process of planning for the worst-case scenario. For example,
 - Develop evacuation *plans* and lockdown *procedures* and *train* for their execution.
- Response is devoted to the steps to take during a crisis. For example,
 - *Notify* emergency responders and *evacuate* building occupants.
- Recovery addresses restoring the learning and teaching environment after a crisis. For example,
 - Assess building integrity and inform students and families, staff, and the community.

Other options can include (Reference 322):

- *Psychological barriers* that provide deterrence through security lighting, fences, and cameras.
- *Physical barriers* such as fences, doors, and locks of all forms and types.
- *Electronic barriers* that detect intruders and initiate an appropriate response. These technological barriers include optical and infrared beams, intelligent cameras, motion-detection systems, and break-glass or open-door detectors.
- *Procedural barriers* that impede the progress of an intruder into a building. Such management procedures can include electronic access controls, metal detectors, and visitor database checks.

2.7 SELECT TECHNOLOGY

General risk literature identifies five traditional methods for treating risks: reduce the risk (e.g., reduce the likelihood or consequence), transfer the risk (e.g., purchase insurance), avoid the risk (e.g., eliminate the activity causing the risk exposure), redistribute the risk (e.g., distribute functions over a range of locations or time), and accept the risk (Reference 322). Because technology is frequently chosen to reduce or avoid security risks, technology cost must be balanced with increased levels of security. Although “risk analysis professionals normally assume that technologies that address the most likely scenarios are wise investments” (Reference 245), school officials should ensure the most appropriate technology is selected based on a well-defined method for evaluating technology that results in solid justification. The technology review (Chapter 3 to Chapter 10) provides factors that can be used to evaluate technology.

When selecting and implementing new technologies or replacing existing technologies, system requirements should be defined. Requirements should map between the risk assessment goals and objectives to ensure the solution chosen will meet the needs of the school or district. The following five factors are an example of factors that could be considered:

- **Range of Use** – What need does the technology usually fulfill? How is it used? How is the technology installed? What are its basic function and capabilities? Are there low-cost alternatives? Are there optional and/or enhanced capabilities?
- **Performance** – What aspects of the technology improve school safety? How are the identified risks reduced by the technology? What are the impacts on policy?
- **Key Technical Specifications** – What are the key technical specifications that the technology must meet to be effective? What environment is the technology designed to operate in? What is the range of the technology's activity or effect? What is the duration of the technology's activity or effect?
- **Cost Considerations** – What are the costs associated with the following areas, respectively:
 - Acquisition
 - Exceptional installation costs (e.g., special wiring)
 - Personnel
 - Training
 - Maintenance
 - Consumables
 - Energy and energy dependency (e.g., backup power)
 - Software licenses
 - System integration (e.g., cameras integrated with alarm systems)
- **Vulnerabilities and Concerns** – What are the concerns for students and staff with disabilities (Americans with Disabilities Act compliance)? Are there privacy concerns? Are there liability and safety concerns? How could the technology be misused? What are the modes of failure? Are there ways to circumvent the technology and enable maladaptive behaviors?

The literature is replete with resources to assist school representatives make this choice. Atlas, for example, poses the following short checklist (Reference 17):

- *What will the system be used for?* Is the intent to prevent intrusion, and if so, to protect the interior or exterior of the building? Who will respond to an alarm and how will they be notified? What should be the delay between trigger and alert for a sensor?
- *What operational aspects of a security system are required, and what is their priority?* What type of alarm system is desired and what is the allowable false alarm or false positive rate? What is the proposed transmission system from sensors to alarms (e.g., radio, hardwired, or Internet)? What is the backup system in power and hardware? How are the alarms assessed (e.g., via camera, combinations of sensors, or investigation by a security officer)? Does the system have tamper alarms, self-tests, or lighting protection?
- *What are the environmental impacts that affect the security system?* Does the system withstand rain and snow or hot and cold temperatures? Does the system require light? Do obstructions, either natural or manmade, impact the ability of the system to operate?

Still other literature takes the approach of matching the security objective—based on the defense-in-depth concept—to the technology choice (Reference 11):

- **Deter** – These technologies discourage undesirable events from occurring, whether the threat is external or internal. These include cameras, man-traps, school resource officers, and other systems.
- **Detect** – These technologies detect and report undesirable events as they happen. These include burglar alarms and physical intrusion detection systems. Such systems typically monitor for indicators of unauthorized activity, such as doors or windows opening, glass being broken, movement, and temperature changes.
- **Prevent** – These technologies physically prevent unauthorized individuals from entering a school building or premises. Locks are a nearly ubiquitous means of securing a building from unauthorized entry.

The architectural and security communities use CPTED, a multi-disciplinary approach to deterring criminal behavior through the built-in, social, and administrative environment.¹⁰ It generally considers site design (e.g., landscaping and other building exterior features), building design (e.g., features such as entrances and lighting), interior spaces (e.g., lobbies, classrooms, administrative areas, and hallways), systems and equipment (e.g., alarms and surveillance systems), and the community context (e.g., community impacts on and from the school) (Reference 17). The following 11 items are representative of the measures commonly found in the literature regarding CPTED and physical security (Reference 115):

- Perimeter fencing to deter trespass and limit access to non-primary entrances
- Single point of entry
- Staff monitoring of arrival and dismissal times
- Visitor management (signs, registration, badges plus escort)
- Vestibule or double entry, with intercom or video call box; visitors must pass through office
- Minimal glass
- Electronic access control
- Video intercoms for visitor screening
- Door hardware
- Panic button in office
- Situational awareness

Figure 2-5 depicts technology choices that a notional school may make to address its security threats.

In addition to the preceding, there are several areas of special concern: cyberspace security, technology integration, and safety planning, which are discussed in Subsections 2.7.1, 2.7.2, and 2.7.3, respectively.

¹⁰ Retrieved 7 April 2016 from <http://www.cpted.net>.

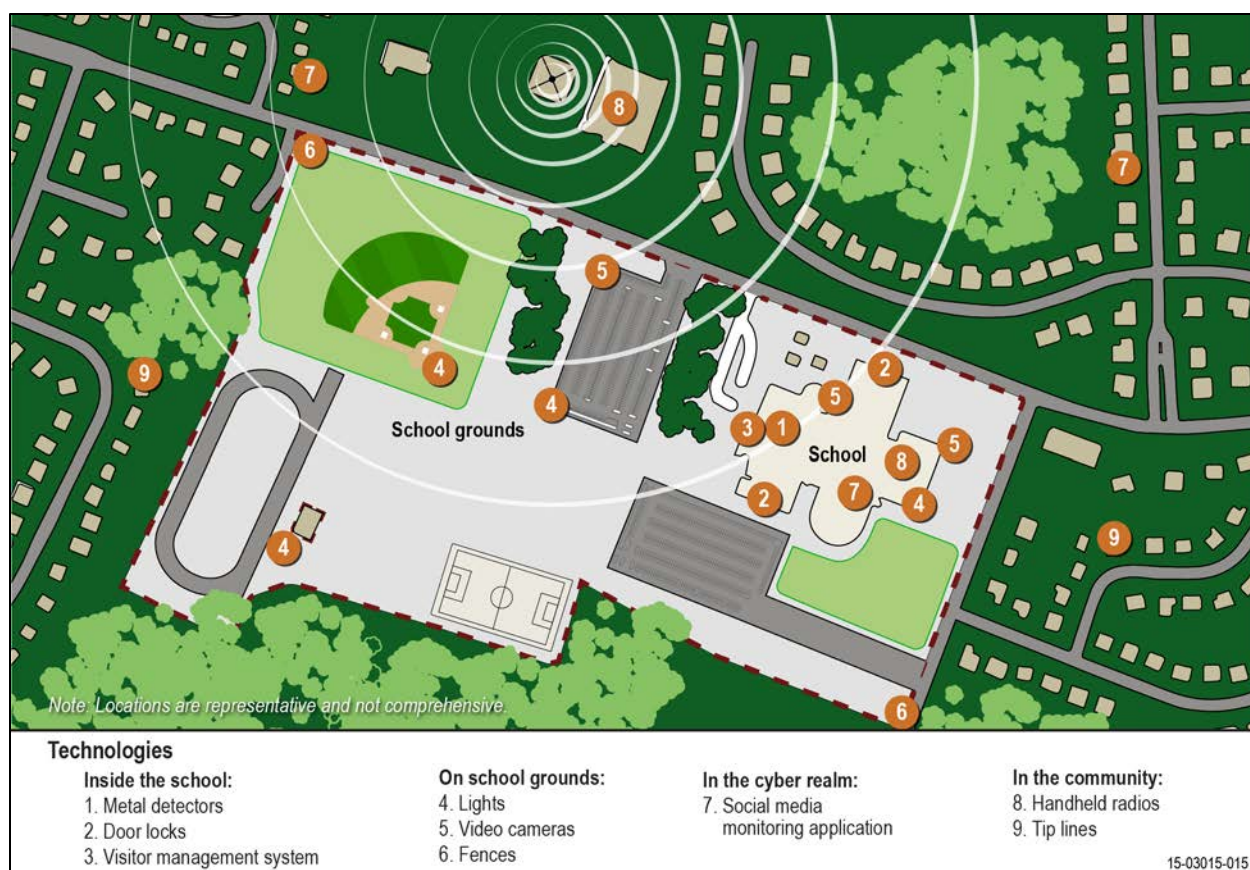


Figure 2-5 Notional Technology Choices

2.7.1 CYBERSPACE SECURITY

Cyberspace involves the online world of computer networks and the Internet, particularly the online behaviors of students when interacting through texting, social media, or other means (as defined in Merriam-Webster¹¹). In addition, cyberspace can provide awareness of potential threats or serve as a vector for the cyber-bully. Schools are increasingly networking their security technologies, just as they rely on online instruction and educational content management tools (Reference 17). However, little is discussed in the literature about securing schools in the cyber realm. Although the information technology field has information about securing the physical systems and the information stored within servers, computers, and other networked assets, tools for securing cyberspace generally remains an area of growing concern with little research.

2.7.2 TECHNOLOGY INTEGRATION

Although the purchase and installation of technology may serve to reduce risk in schools, it is often more effective to deploy and integrate more than one technology. Many technologies are effective in more than one mission area and against more than one risk; therefore, scenario-based planning can reveal overlaps and allow the team to fully implement the capability of a given technology.

¹¹ Retrieved from <http://www.merriam-webster.com/dictionary/cyberspace>

A bank provides a useful, simple example. Typically, to access a bank's vault requires one to pass through multiple layers of protection. For example, after the bank closes for the day, an intruder might have to bypass a locked door and a human guard. Next, the room where the vault resides could be monitored by an infrared camera that is cued to begin recording by a motion sensor. Lastly, if the vault is opened outside office hours, an alarm system may be tripped that sends an alert to local law enforcement and sends a signal to automatically lock the doors. By mixing and matching various security technologies, schools can carry out three objectives of security, prevent, detect, and response (Reference 221).

Integration of combinations of security technologies such as cameras, alarms, communications, and access control devices requires the components' hardware and software to be not only compatible, to maximize their usefulness, but also be fully integrated—they need to be able to “talk” to each other. In other words, these technologies should be able to share data with each other. Integration of various security and information technologies can also be streamlined onto one shared platform, a process known as convergence.

2.7.3 SAFETY PLANNING

Adopting security technologies can greatly reduce a school's or district's risk; however, technology may have significant explicit and hidden costs. Security planning, if conducted in conjunction with technology adoption, can make use of the same risk assessment process¹² and fill gaps not addressed by technology. It should also address any security technologies that have been implemented.

DoED recommends plans that provide an overview of a school's approach to operations before, during, and after an emergency. It outlines the concept of operation, security actions including technology, and training and exercise requirements (Reference 355).

2.8 ITERATE

Once the school or district has implemented safety and security improvements and evaluated their effectiveness, the research should be repeated. Assessments conducted to support technology acquisition and security plans can be used as a starting point for updates and revisions.¹³ Findings from subsequent research cycles can be used to determine whether the security technology has met its goals and objectives. Follow-up research can also determine whether changes at the school are actually making a difference (Reference 242).

Budget requests and investment justification can provide a convenient window of opportunity for periodically repeating the planning process. Subsequent iterations of the planning process may require significantly less time investment. For example, the team membership or school environment description may require adjustment, but a framework is in place. Risks, assets, and vulnerabilities may need to be updated, especially in response to changes in public perception, safety technology improvements, or legal requirements, but plausible examples will be available. In short, the team will be able to evaluate and recommend safety technologies more efficiently once the process is in place.

In summary, an effective risk assessment must be thorough, inclusive, and “living” to the greatest extent possible.

¹² The DHS Planning Process incorporates into Step 2 the actions of “identify threats and hazards; assess risk; prioritize threats and hazards.”

¹³ Ibid

2.9 CONCLUSION

While technology planning is not new, it is an essential component for choosing, justifying, purchasing, and deploying security technologies. Moreover, security technology cannot solve all school security problems; it must be integrated into broader prevention and intervention measures, ranging from security and emergency response plans to crisis response drills to a positive school climate. Greater efficiency, new security options, tighter budgets, and a drive for tighter integration of technologies indicate that the demand for security technology is likely to increase (Reference 17). Choosing the right device or devices is a complex and recurring task. Making effective choices requires decision makers to match goals and objectives with threats, consequences, and vulnerabilities to justify the selection of a technology or suite of technologies. The information provided in this chapter, used in conjunction with the other chapters in this report, should lead to more informed technology acquisition decisions.

2.10 FURTHER READING

Additional resources to consider are:

- ASIS Commission on Standards and Guidelines, ASIS International, *Risk Assessment*, 2015.
- ASIS Commission on Standards and Guidelines, ASIS International, *Security Management Standard: Physical Asset Protection*, 2012.
- DHS Risk Steering Committee, U.S. Department of Homeland Security, *DHS Risk Lexicon*. Washington, DC. 2010.
- Kaye, J., Hill, R., and Goetz, B., *School Emergency Management: A Practical Approach to Implementation*, Polimedia Publishing, 2013.
- National Aeronautics and Space Administration, *NASA Systems Engineering Handbook*, Rev. 1, Hanover, MD, 2007.
- National Clearinghouse for Educational Facilities: <http://www.ncef.org>
- University of Southern Mississippi, National Center for Spectator Sports Safety and Security (2015). *Interscholastic Athletics and After-School Safety and Security: Best Practices Guide*. 1st Edition.

Chapter 3. TECHNOLOGY REVIEW – ACCESS CONTROL

Morgan F. Gaither, MS, and Lauren A. Brush, MS

3.1 INTRODUCTION

The National School Safety Center (NSSC) highlights control of campus access as a central dimension of strategic school preparation (Reference 249). For the purpose of this report, access control devices are defined as devices that prevent or otherwise control physical access to school property, people, and/or resources. Access control devices are some of the most widely used and easily upgraded systems for increasing school security and safety. These devices are valuable in many ways. For instance, they can help ensure school visitors are more easily accounted for and that specialized equipment and other items (e.g., cleaning chemicals, science laboratories) are safely secured.

Because school buildings are physical structures, all schools have in place access control devices of varying sophistication and robustness. This section addresses devices that perform a range of access control functions and covers a number of entry and access methods. For organizational purposes, access control devices are organized into two categories: those that provide a physical barrier and those that provide a way to identify individuals.

It is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district prior to purchasing a safety or security technology. Table 3-1 presents the means by which the study team evaluated access control systems capabilities, aligned with the Federal Emergency Management Agency (FEMA) mission areas: Prevention, Protection, Mitigation, Response and Recovery.¹ This assessment combines the opinion of security subject matter experts and

¹ The preparedness cycle consists of the following five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.
- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

the informed judgment of the authors who evaluated the technologies. Reviewing this table provides a summary of the areas of school security and safety for which access controls may be best suited.

Table 3-1 Access Control Devices – Technology Impact Summary

Access Technology	Prevent	Protect	Mitigate	Respond	Recover
Physical Barriers					
Lock	HIGH Properly installed and used locks can effectively prevent access by intruders	HIGH Properly installed and used locks can effectively protect building occupants from physical access by intruders	MEDIUM Properly installed and used locks can reduce long-term school intrusion vulnerability	LOW Locks may assist first responders in isolating and or locating (in the case of electronic locks) suspects and/or victims	NONE No significant impact on recovery was noted
Fencing	MEDIUM Fencing provides visual indicators of property lines and security measures	HIGH Fencing, especially when paired with surveillance technologies, provides protection against physical intrusion	MEDIUM Properly maintained fencing can reduce vulnerability to physical intrusion	LOW Fencing may help law enforcement and school officials maintain a safe perimeter during an incident.	NONE No significant impact on recovery was noted
Turnstile, man-trap, or one-way door	HIGH Turnstiles and man-traps provide actual and deterrent intrusion prevention	MEDIUM Turnstiles and man-traps provide personnel intrusion protection	MEDIUM Properly maintained turnstiles and man-traps can reduce long-term vulnerability to physical intrusion	CAUTION Man-traps may aid law enforcement efforts to contain a suspect, but may also impede responders and evacuation efforts.	NONE No significant impact on recovery was noted

Table 3-1 Access Control Devices – Technology Impact Summary (Continued)

Access Technology	Prevent	Protect	Mitigate	Respond	Recover
Physical Barriers (Cont'd)					
Vehicle barrier	HIGH Vehicle barriers provide actual and deterrent vehicle collision prevention and traffic control	HIGH Vehicle barriers, especially in styles such as bollards, provide vehicle collision protection for buildings and pedestrian walkways	MEDIUM Properly installed and maintained vehicle barriers can support long-term vulnerability reduction against vehicle collision incidents	LOW May aid traffic control efforts during response.	NONE No significant impact on recovery was noted
Bullet-resistant door	MEDIUM Knowledge of the difficulty of accessing targets may cause a potential shooter to abandon the location	MEDIUM These products may prevent a shooter from injuring people during lockdown	MEDIUM These products may delay an attacker who is attempting to access or injure people through a door	CAUTION These products may prevent first responders from breaching a locked door	NONE No significant impact on recovery was noted
Bullet-resistant window	MEDIUM Knowledge of the difficulty of accessing targets may cause a potential shooter to abandon the location	MEDIUM These products may prevent an attacker from accessing or injuring people through a window	MEDIUM These products may delay an attacker who is attempting to access or injure people through a window	CAUTION These products may interfere with police tactics to disable an attacker or impede efforts to break a window for emergency exit	NONE No significant impact on recovery was noted
Lockdown device	NONE No significant impact on prevention was noted	HIGH When integrated with doors or other systems, these devices interfere with attempts to enter a classroom	HIGH These devices can delay an attacker	LOW May provide some value in methodically assessing and evacuating a crime scene because locked areas can be readily identified as not cleared	NONE No significant impact on recovery was noted

Table 3-1 Access Control Devices – Technology Impact Summary (Continued)

Access Technology	Prevent	Protect	Mitigate	Respond	Recover
Means of Identifying Individuals					
Identification (ID) card	MEDIUM ID cards with specific use and wear policies can deter unauthorized persons and/or make them more easily identifiable by school personnel and students	LOW Traditional ID cards provide minimal protective capabilities	LOW A culture of wearing ID cards and using them for access control may reduce long-term vulnerability to unwanted intrusion	LOW ID cards may be used during an incident to distinguish authorized from unauthorized individuals	LOW The use of ID cards, especially in conjunction with digital locks, may provide some forensics capabilities
<p>Impacts as they relate to a technology's ability to impact a school's ability to <i>prevent, protect, mitigate, respond, or recover</i> from an incident.</p> <p>High: Technology is expected to have a <i>significant</i> impact.</p> <p>Medium: Technology is expected to have <i>some</i> impact.</p> <p>Low: Technology is expected to have <i>little</i> impact.</p> <p>None: Technology is expected to have <i>no</i> impact.</p> <p>Caution: Technology will have an impact; however, it may also have unintended consequences.</p>					

Further details on access control devices are provided in Sections 3.3 and 3.4.

3.2 UTILIZATION STATISTICS

The research team could not find comprehensive statistics on access control systems usage.

3.3 PHYSICAL BARRIERS

Physical barrier devices are those that prevent or control access by entities such as people and vehicles. For the purposes of school security, these include items that facilitate keeping doors closed when necessary, directing pedestrian flow within schools, maintaining control of school property boundaries, and directing and controlling vehicle access into and around school property.

The specific physical barrier technologies discussed in detail are locks, fencing, turnstiles and man-traps, vehicle barriers, bullet-resistant doors and coverings, bullet-resistant windows and films, and lockdown devices.

3.3.1 Locks

3.3.1.1 Introduction



Locks, in particular door locks, are some of the oldest and most commonly used access control devices. Available in varying degrees of sophistication, locks in active use can prevent access to an area or asset

by those not issued a key. Keys can come in a variety of types and sizes and can even be electronic in some cases (see Section 3.4).

The two common lock types, as defined by a leading lock and door hardware vendor,² are cylindrical and mortise. Table 3-2 displays examples of these two lock types.

The Master Locksmiths Association (a United Kingdom-based not-for-profit organization) provides a glossary of locksmith and security terms for those interested in investigating differences in particular lock parts, types of bolts, etc.³

Table 3-2 Examples of Lock Types

Lock Type	Description	Example
Cylindrical	Designed to be installed <i>through</i> the door with a knob or lever on either side that retracts the latch when turned or depressed.	 4
Mortise	Requires a pocket—the mortise—to be cut into the door where the lock is to be fitted; it is common in commercial construction. The parts included in the typical mortise lock installation are: <ul style="list-style-type: none"> • The lock body (the part installed <i>inside</i> the mortise cutout in the door) • The lock trim (which may be selected from any number of designs of levers, handle sets, and pulls) • A strike plate that reinforces the holes placed in the frame into which the latch or deadbolt extends • A keyed cylinder that operates the locking and unlocking function of the lock body 	 5

3.3.1.2 How the Technology Is Used

Locks are used to secure entry to a location by requiring that an individual possess a key or otherwise have internal access. The way a lock is operated by a user is called the lock's function. The American

² <http://locknet.com/lockbytes/excerpts/whats-the-difference-mortise-vs-cylindrical-locks/>

³ <http://www.locksmiths.co.uk/security-advice/security-jargon-buster/>

⁴ http://www.sargentlock.com/products/product_overview.php?item_id=71

⁵ <http://assuredlockanddoorhardware.com/mortise-locks.html>

National Standards Institute (ANSI)⁶ and the Builders Hardware Manufacturers Association (BHMA)⁷ have established standards to govern lock functionality [ANSI/BHMA A156.2 (bored/cylindrical) and ANSI/BHMA A156.13 (mortise)]. ANSI and BHMA have established function codes that identify more than 20 different lock functions, some of which are detailed in Table 3-3. Note that these functions do not include any optional vendor or manufacturer enhancements.

Table 3-3 Lock Function Description Summaries and Codes

Function	Description	Cylindrical ANSI Code	Mortise ANSI Code
Classroom lock	For a classroom, office, or utility room. The key locks and unlocks the outside knob or lever. Inside is always free.	F84	F05
Classroom security	Outer knob and lever are set by the inside key. The outside key operates latch bolt.	F88	F09
Office function	N/A	F109	–
Corridor, dormitory function	Deadlocking latch bolt operated by either a knob or lever. Thumb turn inside throws deadbolt and automatically locks outside knob or lever (anti-panic operation).	F90	F13
Storeroom (closet) lock	Outside knob and level are always rigid. A key is required for entry. Inside is always free-rotating.	F86	F07
Classroom security intruder ⁸	Latch bolt retracted by lever from either side unless outside lever is locked by key from outside. When outside lever is locked, it is unlocked from outside by a key or an operating inside lever. Inside lever is always free for immediate exit.	–	F32
	Latch bolt retracted by key from either side except when outside lever is locked from inside or outside by key. Levers on both sides are always inoperative. Dead bolt retracted by a key from inside or outside. Operating inside lever retracts bolts and unlocks outside.	–	F33
	Latch bolt retracted by key from either side except when outside lever is locked from inside or outside by key. Levers on both sides are always inoperative. Dead bolt retracted by key from inside or outside. Operating inside lever retracts bolts and unlocks outside. Auxiliary latch deadlocks latch bolt when door is closed.	–	F34
Note: Table modified from an Internet Protocol Video Market (IPVM) Information table. ⁹			

⁶ <http://www.ansi.org/>

⁷ <http://www.buildershardware.com/>

⁸ <http://www.i2hardware.com/i2MLClassroomIntruderCutSheetDt082813.pdf>

⁹ <http://ipvm.com/updates/2180>

3.3.1.3 What Makes the Technology Good

3.3.1.3.1 How the Technology Works

The two traditional lock types are defined in Subsection 3.3.1.1.

In addition to coordinating on function codes as described in Table 3-3, the BHMA (accredited by ANSI) develops and maintains performance standards for architectural hardware, including locks, cabinet hardware, sliding and folding doors, spring hinges, exit devices, and more. BHMA identifies three grade levels for this hardware (including locks), with Grade 1 being the highest.¹⁰ The lock's grade is identified by its BHMA product number. For guidance on how to identify the grade via the product number, visit the BHMA website.¹¹ To ensure the greatest level of security and safety, Grade 1 locks should be used in school settings.

3.3.1.3.2 Differentiators

In comparing cylindrical versus mortise locks, installation time and effort may be important factors. Because two holes are drilled straight through the face of the door, a cylindrical lock is more quickly installed than is a mortise lock. A mortise lock requires more time and effort because it requires a “pocket” to be cut into the door.

In consideration of locks such as mortise and cylindrical, enhanced capabilities and other access control technologies like those investigated further in this document should also be considered. Standalone or networked electronic access locks eliminate the need for traditional physical keys, thereby potentially reducing the number of lost or stolen keys and providing enhanced control and access capabilities (see Section 3.4).

3.3.1.3.3 Specifications and Features

Locks provide a significant access control capability. They should be chosen based on the best match with required lock functionality. Several other technical factors are considered in Table 3-4.

3.3.1.3.4 Effectiveness

While locks have been effective and essential access control devices in school for decades, Stafford County in Pennsylvania¹² and the Corvallis School District in Oregon¹³ are two of the many school districts across the United State reevaluating the types, functions (see Table 3-3), and policies associated with their use of door locks. They include options such as policy changes requiring doors to remain closed and locked during classes, using simple and easily removable door stops, or even exchanging existing locks for modern electronic systems. These school districts and many like them are also considering additional lockdown-related devices specific for emergency uses (e.g., mass-shooter scenarios).

3.3.1.3.5 Policy Impacts

Because locks are such an integral component of physical school security, detailed and specific use and access policies should be established and implemented. These policies should be consistent with local

¹⁰ <http://www.buildershardware.com/bhma-standards/grade-levels>

¹¹ <http://www.buildershardware.com/bhma-standards/bhma-product-numbering>

¹² <http://www.securitymagazine.com/articles/83250-securing-doors-in-schools--hospitals-and-detention-centers>

¹³ http://www.oregonlive.com/pacific-northwestnews/index.ssf/2015/11/corvallis_schools_test_new_loc.html

building, safety, and fire codes and should identify the actions that staff and other personnel should take in emergency response scenarios such as active shooters, announced lockdown or shelter-in-place directives, and fire or other emergency evacuations.

Table 3-4 Technical Specification Considerations for Locks

Lock Type	Size and Dimensions	Key Type	Power	Training	Communication and Networking Capabilities
Standard door locks, mortise and cylindrical	Sizes vary depending on type (e.g., dead-bolts, levers, knobs); usually measured by bore size; approximately 3×4 inches for many cylindrical models	Standard key	N/A	Some training on facility-specific locking and unlocking policies and procedures required; minimal training required for physical lock operation	N/A
Electronic locks	Sizes vary; approximately 8×4 inches	Standard key; key or pin pad; electronic key (ID or access) card	Typically standard battery operated; some capable of being hardwired for remote release (9 volts direct current)	Some training on facility-specific locking and unlocking policies and procedures required; some training required for physical lock operation, with complexity depending on electronic lock type	Limited network capability in some models (for remotely controlling access)

3.3.1.4 Concerns About the Technology

3.3.1.4.1 What It Does Not Do

Locks are designed to grant access to persons based on their possession of the appropriate key (whether that is a combination, physical key, electronic access card, fingerprint, etc.). Because locks do not identify or differentiate among people by other means, measures for maintaining positive key control and access or user lists are important for ensuring locks are used appropriately.

3.3.1.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Locks of all varieties are vulnerable to physical tampering and destruction by a variety of means—lock picking, lock removal, lock jamming, etc. Electronic locks may also be vulnerable to electronic tampering. Although lock manufacturers implement hardware to prevent or deter tampering, locks should be regularly inspected and maintained to keep them optimally functional.

3.3.1.4.3 *Possibilities for Misuse*

Although locks are often used to prevent access from unwanted intrusions, a plausible scenario for misuse involves an intruder or other individual first gaining access to an area and then using locks to prevent people from escaping. This scenario may not be preventable in all cases, but having strict key access and distribution policies in place may reduce the potential risk for such actions.

3.3.1.4.4 *Liability and Safety Concerns*

Because all locks have an associated key, another access control vulnerability is introduced when key distribution and key access is not properly controlled. For this reason, school security officials should keep an accurate and current account of those individuals who have keys to areas on school property. Officials should ensure anyone authorized to lock doors (including classroom doors) has ready access to (and knowledge of how to use) keys (including temporary or transient staff such as substitute teachers). Master keys and spare keys should be separately secured to prevent unauthorized people from taking keys. Additionally, records of key access and ownership should be regularly maintained to ensure locks can be re-keyed in the event of key loss or misplacement.

3.3.1.4.5 *Privacy Concerns*

These physical security options do not involve any collection of personal information.

3.3.1.4.6 *Accommodations Needed for Disabilities*

The effects on ingress and egress by people with disabilities should be considered prior to selecting new locks.

3.3.1.4.7 *Other Issues*

No additional issues were identified by the authors.

3.3.1.4.8 *Policy Concerns*

An additional point of consideration when installing locks or developing emergency procedures regarding their use is to ensure compliance with local, state, and/or Federal fire code and other building and safety regulations, including those related to students with disabilities.

3.3.1.5 *Cost Considerations*

As with all technologies, costs should be considered when installing new locks or retrofitting existing access control locations. The costs of locks can vary based on a number of factors. The longer time necessary to properly install mortise locks has been discussed, but other cost factors are described in Table 3-5.

Table 3-5 Lock Cost Considerations

Cost Factor	Cost Description
Acquisition	Locks can range from a few dollars (e.g., padlocks) to hundreds of dollars for electronic and integrated systems.
Installation	Installation costs can vary greatly, with traditional physical locks being less expensive than installation of electronic systems (which may require special wiring and physical modifications to school structures and buildings).
Operation and labor	Labor costs are minimal.
User training	Training costs are minimal for most locks and lock systems; some training may be required for electronic access systems.
Maintenance	Time and personnel costs for lock maintenance. Locks must be properly maintained to function properly, and those not part of an electronic system require individual checks of functionality.
Consumables	Locks must be changed or re-cored, and keys must be replaced when lost or stolen. In addition, resources are required for the tracking of key-holders and for issuing and receiving keys to and from those who require access.
Energy and energy dependency	Electronic locks may have energy dependency (typically battery operated).
Software licenses	Some more sophisticated electronic lock systems may require software for lock integration and control via a central database.
System integration	Some electronic locks can be integrated for remote control and operation.

3.3.1.6 Emerging Technologies and Future Considerations

Classic door (and window) locks are widely used in schools. New electronic locks, including those with biometric reader access (e.g., fingerprint scanners, iris scanners) are increasingly available. Biometric readers employ the use of scanners to identify individuals via biological markers, such as fingerprints, in lieu of ID cards. Biometric locks are commercially available, but this technology is continually developing with increasing capabilities and should be investigated periodically when considering locking devices. Other electronic locking mechanisms include ID cards (see Section 3.4), which usually allow access via embedded electronic components such as radio frequency identification (RFID) chips. Access to electronic locks can be managed via a central computer software program that can also log and identify which locks are accessed and at what time.

In addition to electronic locks, lockdown systems are being explored for use in schools. These systems can be either one-button, hardwired systems that integrate with physical school locks, or electronic notification systems that allow for faster communication about lockdown instructions and initiation. Hardwired systems can provide for immediate lockdown initiation, but can be expensive to install in older schools that would require extensive retrofitting of physical wiring systems. In this case, electronic notification systems, which still require staff to physically lock doors, may be a less costly alternative that will additionally allow for simultaneous notification of local first responders.

3.3.1.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 3-6 presents examples of known lock vendors; however, it is not comprehensive and other vendors may exist. The list is current as of 10 January 2016.

Table 3-6 Lock Vendors

Vendor	Website
Assa Abloy	http://www.assaabloydss.com/en/local/dss/solutions/education-solutions/k-121/
Best Access	http://www.bestaccess.com/
Chown Security	http://www.chownsecurity.com/
Cyberlock, Inc.	http://www.cyberlock.com/
DORMA Americas	http://www.dorma.com/us/en/
Hager Companies	http://www.hagerco.com/
InstaKey Security Systems	http://www.instakey.com/
Medeco	http://www.medeco.com/en/site/medeco/
Marks USA	http://marksusa.com/
Sargent (Assa Abloy)	http://www.sargentlock.com/
Schlage	http://www.schlage.com/en/home.html
Yale (Assa Abloy)	http://www.yalecommercial.com/

3.3.2 FENCING

3.3.2.1 Introduction

Fences are structures used to enclose a specified area. They are constructed of posts with connecting rails and boards or other materials such as wire. Schools routinely use fencing and barricades as a means to control access inside the school building and on school property. Fences can define property boundaries, provide a means of deterrence and delay, and serve as a platform for other security measures. Fence and gates, in conjunction with procedures and other technologies such as photo-electric beam sensors (Subsection 4.3.2), allow the school to positively control who has access to the school grounds.¹⁴

3.3.2.2 How the Technology Is Used

When choosing the type of fencing to install, schools should consider several factors in addition to fence location. The desired level of access control and security, the location of access points such as gates, and the desired visibility and sight lines or privacy are all key considerations.

The American Society for Industrial Security (ASIS) International, an organization of security professionals, authored a *Facilities Physical Security Measures Guideline* (Reference 15). This guideline “outlines eight main categories of physical security measures used to protect facilities: crime prevention through environmental design (CPTED); physical barriers and site hardening; physical entry and access controls; security lighting; intrusion detection devices; video surveillance; security personnel; and

¹⁴ http://www.ameristarsecurity.com/school_security

security policies and procedures.” It identifies a number of recommendations for fencing including height recommendations (e.g., seven feet for medium-security applications) and is an excellent resource to consult prior to installation of new fencing.

3.3.2.3 What Makes the Technology Good?

3.3.2.3.1 How the Technology Works

Fencing comes in a variety of types and materials; each may be best suited for particular applications and possess more or less aesthetic value. Fencing can be categorized by material type or intended use (e.g., vinyl fencing or security fencing). In this document, fencing types discussed will be those identified in a November 2013 Hanover Research report titled *School Fencing: Benefits and Disadvantages* (Reference 148): chain link, welded wire fabric, expanded metal, ornamental, and wood.

Chain-link fencing (Figure 3-1, on left) is versatile and is used in many applications. It is often made of woven steel wire and comes in varying heights, with optional top or bottom bars or wires.

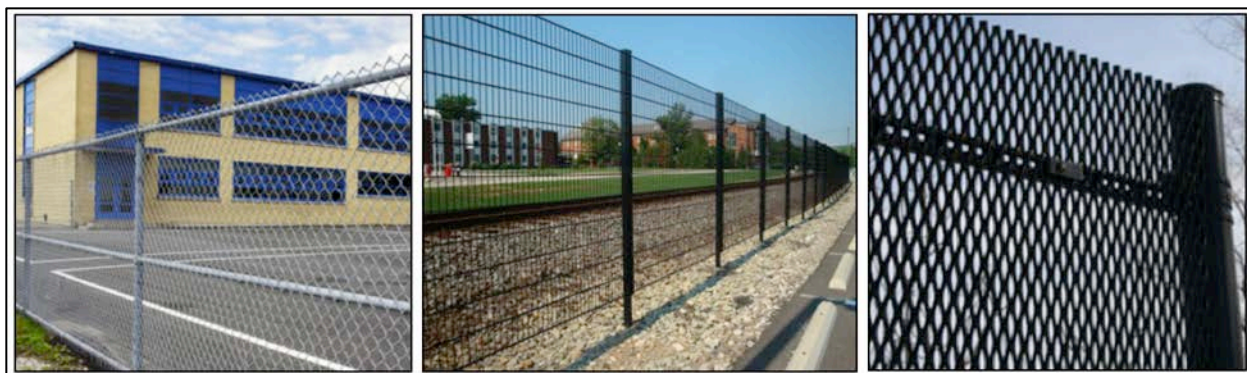


Figure 3-1 Examples of Fences^{15,16,17}

According to Beikon Hardware Group,¹⁸ a welded wire mesh manufacturer, “welded wire mesh fences (like the one in Figure 3-1, in center) are made of high-quality steel, covered with excellent anti corrosion coating...[and] consist of wire mesh fence panel, fence posts, clamps, and bolts.”¹⁹

Expanded metal fencing (Figure 3-1, on right) can be easily identified by the small opening diamond patterns in its panels. Unlike chain-link fencing, which is created by welded intertwining metal wires, expanded metal fences are made from aluminum, steel, or carbon and are created from solid sheets of metal cut and then stretched.

¹⁵ <http://www.chaffinfencing.com/fencing/school-fencing>

¹⁶ <http://www.ametco.com/products/steel-security-fence/welded-wire-fence/>

¹⁷ <http://www.nilesfence.com/faq.php#one>

¹⁸ <http://www.beikonmeshfence.com/>

¹⁹ <http://www.beikonmeshfence.com/Wiremeshfence/weldedwiremeshfence.html>

Ornamental fencing (Figure 3-2, on left) is made of welded iron, steel, or aluminum pickets of varying spacing with or without a top bar. It generally allows greater sight lines, and has increased aesthetic value.



Figure 3-2 Example of Decorative Fences^{20,21}

Wood fencing (Figure 3-2, on right) like ornamental fencing, is created by connecting vertical pickets of varied spacing attached to top and bottom bars. Using wider or more closely spaced pickets or slats makes wood fencing a good option for locations that require a higher degree of privacy.

3.3.2.3.2 Differentiators

Fencing alternatives like shrubs or photoelectric beam sensors do not provide significant physical barriers. Although perhaps less aesthetically pleasing, fencing provides a higher level of physical security and is more easily integrated with surveillance systems such as fiber-optic motion sensor cables, cameras, etc.

3.3.2.3.3 Specifications and Features

Some of the advantages and disadvantages of various fencing types as summarized in the Hanover report are presented in Table 3-7.

²⁰ <http://www.ameristarfence.com/commercial-fence-applications-schools>

²¹ <http://arizonafencebuilders.com/>

Table 3-7 Advantages and Disadvantages of Specific Fencing Materials

Fence Material	Advantages	Disadvantages
Chain link	<ul style="list-style-type: none"> • Least expensive • Easily installed • Maintains visibility 	<ul style="list-style-type: none"> • Easily breached • Targets for vandalism
Welded wire fabric	<ul style="list-style-type: none"> • Difficult to cut • Does not unravel • Less expensive than expanded metal 	<ul style="list-style-type: none"> • More expensive than chain link • Less secure than expanded metal
Expanded metal	<ul style="list-style-type: none"> • Difficult to cut (and climb) • Does not unravel 	<ul style="list-style-type: none"> • More expensive than chain link and welded wire
Ornamental (iron, steel, or aluminum)	<ul style="list-style-type: none"> • Not easily breached or vandalized • Maintains visibility 	<ul style="list-style-type: none"> • Durability and maintenance costs vary greatly
Wood	<ul style="list-style-type: none"> • Appropriate for low-security settings 	<ul style="list-style-type: none"> • May decrease visibility • Inappropriate for locations that require higher security

Although fencing is a popular option for security and visibility reasons, shrubs, trees, and other “living” fences offer a more aesthetically pleasing boundary alternative for delineating school property boundaries for potentially lower cost but also lower security. Heights, densities, and types of vegetation can be chosen based on each school’s perimeter needs. They provide less visibility in some cases (e.g., intruders can hide behind them), but as long as the vegetation is properly maintained, shrubs and trees can be an asset to the look and function of school boundaries.

3.3.2.3.4 Effectiveness

Effective access control and security efforts begin at the perimeter of schools and their property. Appropriately considered fence implementation can potentially deter, delay, and/or prevent unauthorized access and criminal activity. The San Diego Unified School District is one of many school districts across the country evaluating new known security measures. “Since [the] Sandy Hook [school shootings], the district has spent millions of dollars on safety projects, including the fencing.” (Reference 210) The effectiveness of any installed school perimeter or other fence(s) will be determined by factors such as the type and location of the fence, type of behavior targeted, etc.

3.3.2.3.5 Policy Impacts

An additional point of consideration when installing fencing or developing emergency procedures regarding their use is to ensure compliance with local, state, and/or Federal fire code and other building and safety regulations. These regulations may need to be evaluated separately depending on the type and location of the fence. Additionally, local first responders must be informed of key fence and school access points for use during emergency situations.

3.3.2.4 Concerns About the Technology

3.3.2.4.1 What It Does Not Do

Fencing is intended to keep people on one side or the other. Fencing relies upon the effectiveness of access control points to allow authorized students, staff and visitors to pass through the fence. A fence generally will not prevent a criminal from shooting through it or throwing incendiary or explosive devices over it.

3.3.2.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Fencing can provide hand and footholds which allow an intruder to climb the fence in order to access the property. ASIS identifies some guidance concerning fencing, safety, and potential vulnerabilities:

A general rule of thumb is to keep all climbing aids at least 10 feet away from the fence. When that is not possible, additional motion sensors can be added inside the secured perimeter to supplement the sensed fence. These additional sensors will help reduce the risk that an intruder will go undetected after successfully using a climbing aid. ... When surveying the prospective fence site, the contractor and the company should pay particular attention to low-lying areas like drainage ditches, which could allow intruders access. Additionally, drainage areas can also cause erosion, allowing further access to intruders.²²

3.3.2.4.3 Possibilities for Misuse

Schools should be aware that fences potentially create limited sight lines and block natural evacuation pathways. Fencing may be misused in some situations to impede the escape of a potential victim. Fencing which provides privacy for students may also provide cover for undesired activities, such as graffiti or vandalism, either within the fencing or hidden on the opposite side.

3.3.2.4.4 Liability and Safety Concerns

As noted in the Hanover report, “fences may also create safety hazards for students. ...continual fencing can block student pathways, forcing students “to take a longer route where they are more exposed to traffic, crime, or environmental hazards.” (Reference 238) Additionally, failsafe or manual override options should be available for any gates that are operated electronically.

Fencing should be routinely maintained to ensure proper and safe functioning. Fencing with electronic access components should have manual or other override access capability. While striving to maintain security and increase aesthetic value when possible, schools should ensure fences do not impede access for emergency responders.

3.3.2.4.5 Privacy Concerns

These physical security options do not involve any collection of personal information.

²² <https://sm.asisonline.org/Pages/Fence-and-Sensibility.aspx>

3.3.2.4.6 Accommodations Needed for Disabilities

Gate or other fence access points should be located in a way that takes into consideration students with physical disabilities, particularly those who may be in a wheelchair or using other assistance devices. Fencing needs to accommodate ramp access, extra-wide gates, etc.

3.3.2.4.7 Other Issues

No additional issues were identified by the authors.

3.3.2.4.8 Policy Concerns

School officials may want to consider aesthetic appeal and value when choosing a fencing type. Ensuring a school environment that remains accessible and approachable by students is an important factor for many school officials and community members. Some fencing options (e.g., razor wire) promote a less aesthetically pleasing and more institutional-type environment.

3.3.2.5 Cost Considerations

As with all technologies, costs should be considered when installing new or retrofitting existing fencing. The costs of fencing can vary based on a number of factors, as described in Table 3-8.

Table 3-8 Fencing Cost Considerations

Cost Factor	Cost Description
Acquisition and installation	Material type is a major contributor to fencing cost, with chain link and wood being the most economical, and expanded metal and ornamental fencing being more expensive. In addition, fence height impacts costs because higher fences require more physical material for each linear foot installed.
Installation	Minimal, with labor time being the highest cost consideration.
Operation and labor	None
User training	None
Maintenance	Fencing requires regular maintenance, inspection, and occasional repairs. Maintenance and inspection costs can vary greatly.
Consumables	None
Energy and energy dependency	None
Software licenses	None
Integration	Gates could be integrated with other access control systems.

3.3.2.6 Emerging Technologies and Future Considerations

Although not necessarily emerging technologies, alternatives such as decorative shrubs and plants should be considered in cases where security requirements are lower and higher aesthetic value is desirable. Additionally, fences can be supplemented with technologies such as motion sensors and cameras. These technologies can enhance surveillance capabilities by providing additional information about activities surrounding the fenced area such as breeches, etc.

Additionally, a fence alternative (a “virtual fence”) such as a photoelectric beam sensor (Subsection 4.3.2) or camera enhanced with video analytics may be considered to enhance or otherwise replace fencing.

3.3.2.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 3-9 presents examples of known fencing vendors; however, it is not comprehensive and other vendors may exist. The list is current as of 10 January 2016.

Table 3-9 Fencing Vendors

Vendor	Website
A1 Fence Company	http://www.a1fence.com/commercial/
Ameristar Fence (Assa Abloy)	http://www.ameristarfence.com/commercial-fence-applications-schools
Ametco Manufacturing Corporation	http://www.ametco.com/spotlight/
Betafence USA	http://www.betafenceusa.com/School-Fencing
Hurricane Fence Company	http://securityfencecontractor.com/security-fence/security-bollards/
Niles Fence and Security Products	http://www.nilesfence.com/
North American Fence and Railing	http://www.noramfence.com/Automated-Entry-Surveillance/Anti-Terrorism-Barricades

3.3.3 TURNSTILES AND MAN-TRAPS

3.3.3.1 Introduction




Several approaches are available for controlling personnel access to school facilities. This can be accomplished by keeping entrance doors locked, funneling visitors to a single entrance, requiring visitors to sign in, etc. As discussed by Patrick Fiel (Reference 117), “active shooters, registered sex offenders, thieves, vandals, and non-custodial parents often enter a K-12 [kindergarten through 12th grade] campus through the front door. ...Security-conscious schools across the country are taking control of front door access through specific policies and procedures that employ some of the most cost-effective layers of security equipment on the market. Once the front door is secure, the same planning and equipment can help to effectively control access to other school entries.”

More recently, other access control options such as turnstiles and man-traps or vestibules have become available for use in schools. For example, Pennsylvania’s North Penn School District²³ in 2014 completed a \$2.5 million renovation plan that included several secured vestibules for six elementary schools (Reference 123).

Man-traps and turnstiles are personnel access control devices, each with different distinguishing features as displayed in Table 3-10.

²³ <http://www.npenn.org/page/954>

Table 3-10 Examples of Personnel Control Devices

Personnel Access Control Device Type	Description	Example
Man-Trap	A secured space equipped with two or more interlocking doors and a personnel detection system to ensure only one person (or a limited number of people) at a time can pass through into a restricted area. ²⁴ The man-trap tends to be designed like an air lock—a visitor enters through exterior doors, passes into a secured vestibule with locked (bullet-resistant) doors at the other end, and exits through the locked doors once access is granted. ²⁵	 26
Turnstile	Electronic or manual entry control devices often consisting of gates or doors that use mechanical arms and/or optical sensors to limit the number of individuals able to enter at a time (usually only one). They are available in a variety of heights, arm, and door types.	 27  28

3.3.3.2 How the Technology Is Used

Turnstiles come in a variety of types including full height, waist high, and optical (with barrier-free options) (Table 3-10). Full-height models (and revolving doors) provide the highest degree of security, whereas barrier-free optical models provide higher degrees of pedestrian access, while still being able to count and otherwise monitor access. Use of waist-high turnstiles may provide deterrence for intruders while allowing school officials to be more easily aware of intruders; however, they should not be considered for facilities requiring high security as they are easily breached.

As described in *Security Magazine* (Reference 309), “In its most basic form, a man-trap is composed of a set of doors that requires the person to enter the first while the others are closed. Man-traps are typically manual swing doors forming a vestibule but can also use sliding doors or gates. Some man-traps use turnstiles or revolving doors. Once inside the first door, the person cannot pass through the second door until the first door is closed. This system provides security in at least three ways. It makes it difficult to forcibly gain entry by knocking down a single door; it allows time to evaluate the person in

²⁴ http://www.newtonsecurityinc.com/lobby_shield.html#nogo

²⁵ <http://www.tssbulletproof.com/bullet-proof-doors-vs-man-trap/>

²⁶ <http://www.rockdalecitizen.com/news/2015/may/02/four-rockdale-elementary-schools-to-get-new/>

²⁷ <http://haywardturnstile.com/products.cfm>

²⁸ Ibid.

the man-trap before releasing him or her through the second door; and it allows entry of only one person at a time.”

3.3.3.3 What Makes the Technology Good?

3.3.3.3.1 How the Technology Works

As described, turnstiles operate in many ways like a more secure traditional door. These systems default to a “closed” position and allow only one individual at a time to enter an area either through revolving doors or other physical barrier mechanisms. Often, to gain access through a turnstile, ID cards, tickets, or other special keys are required.

Full-height turnstiles (including revolving doors) and man-traps are best suited for high-security facilities because they are not as easily breached as are shorter and/or barrier-free versions. Although turnstiles operate much like more secure traditional doors (i.e., they are a single unit that allows access for only one individual at a time), man-traps and vestibules require a multi-step entrance process. Man-traps are typically two-door entry systems that allow for strictly controlled building access by ensuring an individual is “cleared” to enter a building before unlocking the interior doors(s) to the school.

Man-traps and turnstiles achieve the same objective of access control by different means. Factors such as use scenario, level of security, location, aesthetic impact, and ease of integration into existing structures should be considered when identifying the appropriate solution for use in a school.

Turnstiles, and especially man-traps, can be tied in with visitor management, intercom, video surveillance, Internet Protocol (IP)-based mass notification, IP intercom, and/or duress or distress alarm systems to create a robust personnel access control system network. Additionally, revolving door turnstiles and man-traps can be installed with bullet-resistant doors (and windows) to increase their security value.

Because the installation of these devices can be expensive, schools may choose to implement lower-cost versions or choose alternatives such as locking entry doors, using turnstiles or man-traps only during certain times of day, allowing visitors to enter through only one entrance, and installing cameras and/or doorbell or buzzer options to provide authentication prior to a visitor entering the school.

3.3.3.3.2 Differentiators




Turnstiles are customizable with a number of features. Many more popularly offered capabilities include the ability to be used in single- or dual-direction mode, integration of access card or ticket readers, tail-gaiting (i.e., entrance of more than one person at a time) alarms, unauthorized access alarms, breech or “jump-over” alarms, failsafe or fail-secure modes, remote operation, sleep or energy-saving functions, and manual or automatic arms or barriers.

Because man-traps require specific designs for each individual school or building, they are also highly customizable. Although the main function of a man-trap is to ensure only one person (or specified quantity of people) at a time is authenticated in some fashion prior to being permitted access, this can be accomplished using a number of integrated technologies such as electronic access cards, cameras, metal detectors, computer systems, and biometric access devices.

3.3.3.3 Specifications and Features

Identifying specific authentication requirements will allow for optimal selection of appropriate sensors and alarms for man-traps and turnstiles; however, because each configuration has the potential for unique requirements, the specific vendor should be consulted for design recommendations. Additionally, consider the advantages and disadvantages of the varieties of turnstiles and man-traps presented in Table 3-11.

Table 3-11 Advantages and Disadvantages of Turnstiles and Man-Traps




Type	Advantages	Disadvantages	Approximate Dimensions	Photo Example
Waist-high turnstile (traditional)	Provides security deterrent; provides ability to slow down personnel throughput; single or dual direction	Can be jumped or breeched easily	Height: 39 in. Width: 37 in. Depth: 9 in. Arm length: 15 in.	 29
Waist-high turnstile (optical, barrier-free)	More aesthetically pleasing; capable of handling higher throughput rates; potentially smaller physical footprint; single or dual direction	Can be breeched easily; more costly than traditional turnstiles	Height: 39 in. Width: 35 in. Depth: 9 in.	 30
Waist-high turnstile (optical, barriers)	Provides security deterrent; provides ability to slow down personnel throughput; more aesthetically pleasing; single or dual direction	Can be jumped or breeched easily	Height: 39 in. Width: 49 in. Depth: 13 in. Arm length: 12 in.	 31

²⁹ <http://haywardturnstiles.com/lc100.cfm>

³⁰ <http://www.smartersecurity.com/entry-security/barrier-free-turnstiles>

³¹ <http://www.boonedam.us/product/security-access/optical-turnstile/speedlane-300>

Table 3-11 Advantages and Disadvantages (Continued)

Type	Advantages	Disadvantages	Approximate Dimensions	Photo Example
Full-height turnstile	High level of security; single or dual direction; available in single or tandem units	Less aesthetically pleasing for use in schools	Exterior height: 91 in. Interior height: 84 in. Diameter: 96 in. Clearance: 30 in.	 32
Full-height turnstile (revolving doors)	More aesthetically pleasing than traditional full-height metal turnstiles; when left to freely rotate, can handle higher through-put; can save on heating and energy costs due to design	Immediate access to school interior (like a standard door); requires more maintenance than standard door; more costly to install and purchase	Exterior height: 91 in. Interior height: 84 in. Diameter: 72 in. Clearance: 30 in.	 33
Man-traps and vestibules	High level of security; easily integrated with other security technologies	Low throughput; by design, usually one person can enter at a time; may need frequent maintenance; more costly to purchase and install	Highly variable	 34

3.3.3.3.4 Effectiveness

Man-traps and turnstiles are most often found in secured facilities like banks, government buildings, and infrastructures like stadiums. Some turnstiles can accommodate higher rates of throughput, but man-traps are not designed to accommodate large throughput rates and therefore should not be used for screening the large number of authorized individuals arriving at a school during normal arrival and departure times.

³² <http://www.alvaradomfg.com/secured-entry-control-products/>

³³ <http://www.intlenrance.com/titan.htm>

³⁴ <http://www.computersecurity.org/physical-security-cybersecurity-information/man-traps/physical-security-installing-man-trap-air-lock-access-control-systems/>

3.3.3.3.5 *Policy Impacts*

Schools should establish and publicize expectations and procedures for any students, staff, teachers, or visitors expected to use the systems. Emergency response policies should reflect appropriate actions to ensure that egress during emergencies can be accomplished in a timely manner and that when necessary, the turnstiles and man-traps can be closed or locked.

3.3.3.4 *Concerns About the Technology*

3.3.3.4.1 *What It Does Not Do*

Man-traps and turnstiles prevent or slow physical access, and in some cases may assist in initiating response to unauthorized individuals (through use of alarms, etc.), but these devices do not respond to immediate threats such as persons with active weapons, explosives, etc.

3.3.3.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

Several vulnerabilities may exist with any chosen turnstile or man-trap. As previously noted, waist-high turnstiles (including those with alarms) can be physically breeched more easily than full-height models. Full-height turnstiles can still provide security, deter crime, prevent tailgating (i.e., more than one person enters at a time), and control or direct access in appropriately chosen locations.

3.3.3.4.3 *Possibilities for Misuse*

The research team did not identify any misuse scenarios for this technology.

3.3.3.4.4 *Liability and Safety Concerns*

In an article for *The Data Center Journal*, Jeff Clark notes two major concerns with man-traps (and turnstiles) (Reference 64): “One major concern with man-traps [and turnstiles] is safety. To avoid a dangerous situation in the event of a fire or other disaster, the man-trap [turnstile] must allow an individual to exit into the non-secure area. This may, of course, trigger an alarm, but the individual cannot be forcibly detained—for fire-hazard and other reasons.”

3.3.3.4.5 *Privacy Concerns*

These physical security options do not involve any collection of personal information.

3.3.3.4.6 *Accommodations Needed for Disabilities*

The effects on ingress and egress by people with disabilities should be considered prior to selecting this technology. Clark also states: “man-traps [and turnstiles] must be built large enough to comply with U.S. Americans with Disabilities Act regulations, allowing disabled personnel to use them.” (Reference 64)

3.3.3.4.7 *Other Issues*

No additional issues were identified by the authors.

3.3.3.4.8 Policy Concerns

When installing access control devices or developing emergency procedures regarding their use, school systems must ensure compliance with local, state, and/or Federal fire code and other building and safety regulations, including those related to students with disabilities.

3.3.3.5 Cost Considerations

Like other access control technologies, the costs associated with these personnel entry systems can vary depending on the type of system chosen and the degree of security desired. Integration of complementary technologies (such as alarms, cameras, etc.) will increase the cost above standard systems. Table 3-12 lists estimates for initial purchase of single units.

Table 3-12 Estimated Purchase and Installation Costs for Turnstiles and Man-Traps

Turnstile Type	Purchase Cost (per lane or unit)*
Waist-high turnstiles (traditional)	\$2,000 to \$10,000 ³⁵
Waist-high turnstiles (optical, barrier-free)	\$5,000 to \$10,000 ³⁶
Waist-high turnstiles (optical, barriers)	\$15,000 to \$70,000 ³⁷
Full-height turnstiles	\$3,500 to \$15,000 ³⁸
Man-traps and vestibules	\$30,000 to \$150,000 ³⁹

*These costs are only estimates. Actual costs will vary depending on vendor, installation requirements, necessary building reconfiguration, etc.

Purchase costs are only the initial costs associated with these devices. Other cost considerations are presented in Table 3-13.

Table 3-13 Man-Trap and Turnstile Cost Considerations

Cost Factor	Cost Description
Modification and installation	Some of the devices identified, particularly man-traps, may require significant modification to existing building structure(s) and may require that other existing entrances be locked or otherwise inaccessible to individuals.
Operation and labor	None, unless it is a manned entrance.
User training	School security officials, administrators, and others will need routine training on the use of these personnel-access devices including any emergency procedures.

³⁵ <https://turnstilesnow.com/store/waist-height-turnstiles.html?p=1>

³⁶ <http://www.turnstiles.us/>

³⁷ <http://www.smartersecurity.com/entry-security/barrier-turnstiles/fastlane-glassgate-200-turnstiles>

³⁸ <http://www.turnstiles.us/>

³⁹ <http://www.schoolnewsnetwork.org/index.php/2014-15/schools-spend-big-tighten-security-we-live-different-world/>

Table 3-13 Man-Trap and Turnstile Cost Considerations (Continued)

Cost Factor	Cost Description
Maintenance	Turnstiles and man-traps need routine maintenance to ensure they are functioning properly. More complex devices (including those with additional integrated technologies) require regular tuning, calibration, and testing. In the case of man-traps, which are more complicated multi-layer devices, the failure of a single component (e.g., alarm, lock) can render the device inoperable or ineffective.
Consumables	Lubrication
Energy and energy dependence	Man-traps will require electricity and an ability to exchange information regarding access. If turnstiles have a counting function, they may require access to electricity and connectivity to a database.
Software licenses	If connected to access control, it may require software.
System integration	Some features of turnstiles and man-traps require the ability to integrate with other security technology.

3.3.3.6 Emerging Technologies and Future Considerations

Man-traps can provide the capability to carefully control personnel access, particularly visitors. Man-traps and vestibules can be integrated with a number of additional technologies such as cameras, biometric readers and scanners, and metal detectors. As each of these technologies evolves and their capabilities become enhanced, their use with man-traps should be reevaluated.

3.3.3.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 3-14 presents examples of known vendors of turnstiles and man-traps; however, it is not comprehensive and other vendors may exist. The list is current as of 10 January 2016.

Table 3-14 Turnstile and Man-Trap Vendors

Vendor	Website
Alvarado	http://www.alvaradomfg.com/
Boon Edam	http://www.boonedam.us/products-and-services/security-doors-portals
Coastal Security Solutions	http://coastalsecuritycorp.com/
Controlled Access, Inc.	http://www.controlledaccess.com/
Hayward Turnstiles	http://haywardturnstile.com/
International Entrance Control	http://www.intlentrance.com/
Newton Security	http://www.newtonsecurityinc.com/
P&M Doors	http://pandmdoors.com/
Perey Turnstiles	http://www.turnstile.com/
Porta-King Building Systems	http://www.portaking.com/
Smarter Security	http://www.smartersecurity.com/
Stanley	http://www.stanleyaccess.com/commercial-entry-doors

3.3.4 VEHICLE BARRIERS

3.3.4.1 Introduction

Vehicle barriers protect buildings against vehicle collisions (both purposeful and inadvertent), control vehicle traffic, protect pedestrian walkways, and generally control the location and/or speed of vehicles in an area. They are available in a variety of styles including bollards⁴⁰ (Figure 3-3, on left) and barricades⁴¹ (Figure 3-3, on right).



Figure 3-3 Examples of Vehicle Barriers

Jennie Morton of Buildings.com, a site (and magazine) run by facility managers and business owners that focus on facility management news and research, notes that “there are hundreds of [vehicle barriers] that can be specifically tailored to your facility. Common barriers include wedges, plates, drop arms, bollards, crash and sliding gates, and cabling systems. These can be manual or automated, surface or foundation mounted, hydraulic or pneumatic, and portable or permanently installed.” (Reference 225)

3.3.4.2 How the Technology Is Used

Vehicle barriers serve to direct traffic flow and to protect pedestrian walkways, buildings, and structures from vehicle collision.

Permanently installed vehicle barricades are an effective end solution for applications that require a high level of security. Often installed directly in vehicle access points such as parking lot entrances, high-security vehicle barricades are made of steel, are installed under or with concrete, and can be raised and lowered electronically or pneumatically.

Vehicle bollards can be equally effective in high-security applications. They can be installed in sidewalks and other pedestrian-accessible areas and, like vehicle barricades, can be retractable.

When considering the installation of vehicle barriers at a school, several factors will determine the most effective end solution. In two articles written for the *Whole Building Design Guide*⁴² (a program of the National Institute of Building Sciences), Dr. Charles Oakes identifies issues, concerns, and relevant codes

⁴⁰ <http://securityfencecontractor.com/security-fence/security-bollards/>

⁴¹ <https://deltascientific.com/high-security/surface-mounted-barricades/tw2015-surface-mounted-barricade/>

⁴² <https://www.wbdg.org/>




and standards for non-crash and attack-resistant bollard models (Reference 258) and for crash and attack-resistant models (Reference 259).

As noted by Dr. Oakes, there are several factors to consider:

- Use location(s) (facility entrance, parking lot, pedestrian sidewalk, etc.)
- Desired level of security and protection (protection against vehicle crashes at designated speeds, deterrence or traffic guidance only, etc.)
- Level of permanence of barriers (removable and permanent installation options are available)
- Desired level of aesthetic value (like fencing, varying degrees of aesthetically pleasing options are available)

Table 3-15 presents some of the available barricade and bollard options.

Table 3-15 Examples of Vehicle Barriers






Barrier Type	Material	Permanent?	Protection Level	Example
Vehicle bollard	Plastic	No	Usually only a deterrence or for traffic-control purposes	 43
	Concrete	Yes	Can provide some vehicle crash protection	 44
	Metal or steel	Yes, can be fixed or retractable	Provides vehicle crash protection	 45

⁴³ http://www.bunnings.com.au/whites-on-site-1050mm-pvc-safety-bollard-with-5kg-base-_p1090296

⁴⁴ <http://www.markstaar.com/QUICK-SHIP-Round-Concrete-Bollard-w-Reveal-Line-TF6010QS.html>

⁴⁵ <http://www.ameristarsecurity.com/security-bollards/manual-bollards>

Table 3-15 Examples of Vehicle Barriers (Continued)

Barrier Type	Material	Permanent?	Protection Level	Example
Vehicle barricade	Plastic	No	Usually only a deterrence or for traffic-control purposes	 46
	Metal	Yes, can be fixed or retractable	High level of anti-crash protection	 47
Vehicle barricade (gate)	Plastic	No	Usually only a deterrence or for traffic-control purposes	 48
	Metal	No	Usually only a deterrence or for traffic-control purposes	 49
	Metal	Yes	Can have minimal anti-crash protection	 50

The examples in Table 3-15 represent a small sample of the available vehicle barrier options. Barricades and bollards both have extensive potential for enhanced or upgraded protection and other security capabilities. They can be supports or good collocations for other types of access control and security technologies such as cameras, lighting, manned security stations, etc. Other vehicle-related technology such as tire-compromising devices (e.g., spike strips) can be installed in addition to vehicle barriers to deter and prevent unwanted vehicle access.

Removable plastic bollards and traffic cones are examples of lower-cost and less crash-resistant options often used for temporary traffic- and pedestrian-control purposes. Curved driveways and entrances may help to calm or slow approaching traffic, and large concrete planters can serve as more aesthetic bollards (Figure 3-4).

⁴⁶ <http://www.perimetersecurityproducts.com/products/42%E2%80%B3-x-8%E2%80%B2-positive-lock-safety-barricade-standard-economy/>

⁴⁷ <http://www.facilitiesnet.com/buildingproducts/details/Vehicle-Barricade-Delta-Scientific--1167>

⁴⁸ <https://starttraffic.com/temporary-plastic-barricade-avalon-pedestrian-barrier>

⁴⁹ <http://www.stanchiondepot.com/barricade-purpose.html>

⁵⁰ <http://www.campusafetymagazine.com/article/Get-Into-the-Swing-of-Parking-Access-Control>



Source: Red River Mutual⁵¹

Figure 3-4 Example of a Concrete Planter Vehicle Barrier

3.3.4.3 What Makes the Technology Good?

3.3.4.3.1 How the Technology Works

As noted in the article by Jennie Morton, benefits to vehicle barriers include the following (in addition to serving as an immediate deterrent to criminals):

- Create a choke point.
- Reduce traffic speed and density.
- Increase safety of pedestrians.
- Allow guards to conduct searches.
- Repel speeding vehicles.

3.3.4.3.2 Differentiators

Vehicle barriers serve a specific physical access prevention-and-protection function that is unlikely to be served by other technologies or devices. If vehicle surveillance and tracking are also desirable functions, other technologies such as cameras and photoelectric beam sensors could be integrated into the barriers or used in lieu of them.

3.3.4.3.3 Specifications and Features

Dr. Oakes recommends the use of two checklists developed by the National Clearinghouse for Educational Facilities (NCEF),⁵² a program of the National Institute of Building Sciences, when planning and designing the use of bollards and barriers in schools:

- Outdoor Athletic Facilities and Playgrounds checklist,⁵³ which addresses natural surveillance, boundaries and setbacks, and separation from vehicular traffic

⁵¹ <https://www.redrivermutual.com/loss-prevention-program/loss-prevention-safety-tips/commercial-safety/preventing-vehicle-impact-to-buildings/>

⁵² <http://www.ncef.org/>

⁵³ http://www.ncef.org/pubs/MH/outdoor_athletic.pdf

- School Ground and Site Access Control checklist,⁵⁴ which covers (more broadly) a spectrum of areas such as site surveillance, site territoriality and maintenance, site access control, school surroundings, high risk sites, landscaping, traffic circulation, and vehicle parking, among others

3.3.4.3.4 Effectiveness

The use of vehicle barriers is mentioned in a number of traffic-calming and other design guides, and these devices are used routinely around critical infrastructure and important assets such as Federal buildings and public transit (e.g., subway entrances). Although the research team did not find many real-world examples of vehicle barriers preventing vehicle crashes at schools, the lack of vehicle access controls is specifically noted in the *2013 K-12 School Security Practices Guide* from the Department of Homeland Security:

The layouts of most schools and school grounds permit close proximity of vehicles to buildings and areas where students congregate. These include parking areas, driveways on school grounds (including long avenues of approach for bus access), and nearby streets. Some schools have no vehicle barriers near the main entrances, other vulnerable parts of the buildings, or student gathering areas.

Referencing a 2003 FEMA effort, FEMA 429, “Primer for Design Safe Schools Projects in Case of Terrorist Attacks,” Dr. Oakes notes:

FEMA in 2003 conducted a cost-benefit analysis of 43 strategies to provide safety to school campuses (see FEMA 428, page 2-29). These were arranged on an ordinal scale progressing from “less protection/less cost/less effort” strategies on the lower end of the scale to “greater protection/greater cost/greater effort” strategies at the upper end of the scale. Of the 43 strategies, seven could be met with the use of bollards. Despite the fact that bollard cost remains relatively constant from one application to another, three of the higher cost quartiles included two bollard strategies each, and the least cost quartile had one bollard application. The conclusion is that costly high demand strategies can be met with low cost bollards.

3.3.4.3.5 Policy Impacts

An additional point of consideration when installing access control devices or developing emergency procedures regarding their use is to ensure compliance with local, state, and/or Federal fire code and other building and safety regulations including those related to students with disabilities.

3.3.4.4 Concerns About the Technology

3.3.4.4.1 What It Does Not Do

Vehicle barriers designed for traffic control (such as cones) may not be designed or rated to stop vehicle ramming or other attacks. Additionally, barriers intended for anti-ramming purposes are designed and tested for a certain type and speed of impact. Other types of attacks or those that occur outside of the design boundaries may cause the barrier to fail. When not part of a staffed system, vehicle barriers do not differentiate between authorized and non-authorized persons, and will not prevent such persons from gaining access via stolen access cards, etc.

⁵⁴ <http://www.ncef.org/pubs/MH/grounds.pdf>

3.3.4.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

In addition to the design features discussed, electronically or pneumatically controlled systems may be vulnerable to intentional tampering or mechanical or electrical failure. Portable vehicle barriers are especially vulnerable to being moved, stolen, vandalized, or otherwise tampered with.

3.3.4.4.3 *Possibilities for Misuse*

As discussed, vehicle barriers could be misused to negatively impact traffic flow or otherwise block access (e.g., barriers that are moved without authorization). Electronic or integrated and in-ground models may be used similarly if unauthorized personnel gain access to controls via stolen ID cards or other means.

3.3.4.4.4 *Liability and Safety Concerns*

A major concern when installing vehicle barriers is the need to maintain access for emergency vehicles. Although the purpose of vehicle barriers is usually to keep vehicles out of areas, during fires and other emergencies, first-responder vehicles need to be able to access the school in a timely fashion. Local and national fire codes and any other relevant regulations should be considered when planning for emergency vehicle access. Additionally, plans should include manual overrides or failsafe options to facilitate access for first responders.

3.3.4.4.5 *Privacy Concerns*

These physical security options do not involve any collection of personal information.

3.3.4.4.6 *Accommodations Needed for Disabilities*

The effects on ingress and egress by people with disabilities should be considered prior to selecting this technology. Specifically, accommodations for physically disabled support devices such as wheelchairs, wheelchair lifts, etc., should be considered when planning and installing vehicle barriers.

3.3.4.4.7 *Other Issues*

No additional issues were identified by the authors.

3.3.4.4.8 *Policy Concerns*

Like fences, vehicle barriers, especially large, automated, in-ground systems, may not be aesthetically pleasing and can create a more institutional-like environment at school. This possibility should be considered during the selection and placement of any installed vehicle barriers.

3.3.4.5 *Cost Considerations*

For most types of vehicle barriers, initial acquisition cost is the major factor in the purchase of the device, but in more sophisticated in-ground models, installation costs may also be significant (Table 3-16).

Table 3-16 Vehicle Barrier Cost Considerations

Cost Factor	Cost Description
Acquisition	Bollard and barricade options costs range from less costly removable plastic bollards to more expensive in-ground retractable bollards and barricades.
Installation	Permanent retractable options that involve installation underground or in concrete can be costly, depending on the amount of underground structure or retrofitting required.
Operation and labor	Some operation and labor costs may be involved for vehicle barriers that are portable or moveable and for those requiring manned operations (such as lift-gate barrier with a guard booth in lieu of electronic access).
User training	School security and other relevant staff should be periodically trained in the use and manual override (if available) of any vehicle barricade capability.
Maintenance	Some of the more sophisticated barrier devices require routine oil changes to maintain desired performance; less sophisticated versions (like concrete planters) require little maintenance other than occasional cleaning and/or debris removal. Additionally, damaged barriers will need to be replaced to maintain the desired level of protection.
Consumables	None
Energy and energy dependency	Most electric or pneumatic versions require little energy use.
Software licenses	None
System Integration	Some electronic gates may be integrated into other access control systems (e.g., ID card readers).

3.3.4.6 Emerging Technologies and Future Considerations

In-ground vehicle barriers may not be practical or cost-effective devices for many schools. Schools may find bollards and large concrete planters more cost-effective and aesthetically pleasing alternatives for protection from vehicle collisions, whether deliberate or accidental. The research team did not identify any newly specialized vehicle barrier technology, but recognizes that technologies for this specialization may emerge in the future.

3.3.4.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 3-17 provides examples of known vendors of vehicle barriers; however, it is not comprehensive and other vendors may exist. The list is current as of 10 January 2016.

Table 3-17 Vehicle Barrier Vendors

Vendor	Website
Ameristar Security Products	http://www.ameristarsecurity.com
Detla Scientific Corp.	https://deltascientific.com/
Hurricane Fence Company	http://securityfencecontractor.com/security-fence/security-bollards/
North American Fence and Railing	http://www.noramfence.com/Automated-Entry-Surveillance/Anti-Terrorism-Barricades
Perimeter Security Products	http://www.perimetersecurityproducts.com
Star Traffic	https://starttraffic.com/barricades
Traffic Guard Direct	http://www.trafficguard.net/applications/schools/

3.3.5 BULLET-RESISTANT DOORS AND COVERINGS

3.3.5.1 Introduction

Bullet-resistant doors, often called *bullet-proof* doors, are security doors constructed from materials designed to prevent bullets from passing through them. Bullet-resistant coverings are plate-like panels installed over existing doors, using screws or adhesives, to increase their resistance to penetration by bullets. Such products may also provide added protection from flying debris in the event of a bomb detonation.

For the purposes of this report, there are several technology-specific terms associated with these systems:

- **Bullet proof:** Capable of preventing penetration by a bullet fired from a firearm. Because the force of a bullet is highly variable depending on factors such as the type of firearm, type of projectile, and distance from muzzle to target, items meant to be *bullet proof* are best described as *bullet resistant*.
- **Bullet resistant:** Capable of preventing penetration by some types of projectiles, but may allow penetration when subjected to repeated strikes or to higher-powered projectiles. Bullet resistance should be specified in terms of an accepted standard such as National Institute of Justice (NIJ) 018.01 or American Society for Testing and Materials (ASTM) F-1233 (Nationwide Structures, Inc.).
- **Light:** A glass window cut into the center of a door primarily made of a non-glass material such as wood or metal (shown in the two doors on the left in Figure 3-5).
- **Sidelight:** A narrow vertical window along the right or left side of a door (shown in the two doors on the right in Figure 3-5).



Note: Placing the sidelight away from the door handle (as shown in the far right door) makes it more difficult after breaking the glass to reach through to unlock the door.

Figure 3-5 Examples of Doors with Lights and Sidelights

3.3.5.2 How the Technology Is Used

Exterior school doors are primarily intended to secure building contents against theft and vandalism, and thus are generally designed to withstand forcible entry by a potential intruder attempting to break through the door surface, smash the lock mechanism, or remove the door from its frame. However, traditional exterior doors are not intended to resist gunfire. This introduces the danger that an armed assailant can shoot the door either to damage it enough to force entry or to injure people inside by shooting through the door. Bullet-resistant doors are most often used in schools to provide protection at the front entrance. In combination with bullet-resistant glass, this provides a way for occupants to see a potential intruder, safely initiate a lockdown, and notify police.

Interior classroom, office, and bathroom doors are traditionally used to minimize noise and distractions, provide privacy, and limit the spread of fire. Local fire codes rather than security concerns often determine the construction of interior doors and their closure mechanisms. Faced with the need to protect students from threats inside the building, interior doors have become an integral part of school security plans.

During a lockdown, interior doors are locked to allow occupants to remain safely inside a room until the threat can be identified and removed from the school. Doors with secure frames and locks can protect the occupants from an intruder, but unless the doors are bullet resistant, they may not protect occupants from bullets shot through the door. Some interior doors have glass panes to allow light into the rooms and hallways. Glass used in or near doors is normally tempered glass, which breaks into small blunt-edged pieces instead of large shards capable of cutting people. Some windows have embedded wire mesh to impede an intruder attempting to reach through and manually unlock the door or to pass bodily through a window with a large enough frame, but an intruder could still fire a weapon through the mesh at anyone sheltering in the room.

3.3.5.3 What Makes the Technology Good?

3.3.5.3.1 How the Technology Works

Bullet-resistant doors for exterior use are made of aluminum or steel with glass-clad polycarbonate windows. Bullet-resistant doors can also be made of heavy acrylic, but this material must be at least one inch thick to be considered bullet resistant⁵⁵ and is therefore generally only used for bullet-resistant transaction windows.

Bullet-resistant coverings are armored plates attached to the door using screws or industrial adhesives. They are used to increase the resistance of the door material or to cover a door light to provide additional protection for room occupants (Figure 3-6).



Photo: Campus Security Systems. The option on the far right includes a hinged section used to cover the door light during lockdown.⁵⁶

Figure 3-6 Samples of Bullet-Resistant Panels, with Corkboard and Dry Erase Board Surfaces, Attached to Standard Doors

3.3.5.3.2 Differentiators

Cost is a deciding factor when making the initial decision between adding bullet-resistant covers to existing interior doors and replacing them with bullet-resistant doors. Schools should evaluate their doors, frames, and locks to determine whether existing structures are robust enough to resist the force exerted by a determined attacker. Neither bullet-resistant doors nor door coverings will provide the intended safety benefit if the door hangs in a structurally weak doorframe or has an easily breached

⁵⁵ Wikipedia (7 September 2015) "Bulletproof glass." Retrieved 9 November 2015 from https://en.wikipedia.org/wiki/Bulletproof_glass

⁵⁶ http://www.hardwirellc.com/products/school_office/door.htm

lock. If doorframes and locks must be replaced, it is possible that bullet-resistant doors that include hardened frames and locks to prevent a locked door from being kicked open will be more cost effective.

3.3.5.3.3 *Specifications and Features*

The weight of the door or covering may also be an issue in older buildings. Building structures must be able to support the added weight without allowing the doors to sag. The weight of metal bullet-resistant doors generally requires reinforced walls and ceiling supports (Reference 345).

The vendor must be able to supply the results of independent tests indicating the standard met by the product. A search for products revealed some that offer up to NIJ Level IIIA, which is described as capable of stopping five 240-grain, lead, semi-wadcutter gas checked rounds from a .44 magnum or five 124-grain, full metal jacket rounds from a 9-mm weapon. Schools should consult with local law enforcement to understand the types of weapons used in local crimes and in school shootings around the nation to make an informed decision about the level of bullet resistance needed.

When considering a product to increase bullet resistance of interior doors, the level of resistance offered by the door or covering is an important factor. Several organizations have developed standards used to certify the bullet resistance of materials. Some rating systems, such as the U.S. State Department SD-STD-02.01, European Standard Deutsche Institut für Normung (DIN) EN 1063, British Standards Institution BS 5052, and German DIN 52-290, specify the bullet-resistant rating by indicating the type of firearm and projectile blocked by the material. The Underwriters Laboratories (UL) 752 and NIJ 018.01 rating systems use a series of numbered levels with a higher number indicating the ability to resist more powerful projectiles. Regardless of the system, all ratings are based on the ammunition type, weight of the projectile, force of the projectile, and number of shots to which the test object was subjected.⁵⁷

3.3.5.3.4 *Effectiveness*

There have been numerous incidents of people injured or killed by bullets fired through a closed door. Professor Liviu Librescu was fatally shot through a door during the Virginia Tech attack (Reference 372), and two students were killed in Erfurt, Germany, when an attacker fired through a locked door.⁵⁸ However, no literature was found indicating operational performance of bullet-resistant door panels in an actual emergency.

Bullet-resistant doors and coverings are intended to slow or prevent a determined shooter from injuring people on the other side of the door. Before implementing new doors or coverings, existing doors, frames, and locks should be evaluated to determine whether they are structurally sound enough to prevent access and to hold the weight of new doors or coverings. An evaluation of the overall building structure is also recommended to ensure ceiling structures and doorframes can support the added weight (Reference 346). Consider which doors will provide the most safety benefits. For example, if the school has wings or areas separated by doors, replacing these doors can effectively protect everyone in the area. Also evaluate exterior doors and consider strengthening them, as needed.

⁵⁷ Nationwide Structures, Inc. n.d. "Ballistic Charts." Retrieved 2 September 2015 from <http://www.nationwidestructures.com/ballistic-key.html>.

⁵⁸ Wikipedia, "Erfurt Massacre," 19 September 2015. Retrieved 8 October 2015 from https://en.wikipedia.org/wiki/Erfurt_massacre

3.3.5.3.5 *Policy Impacts*

The installation of new doors or door coverings may require modification to existing emergency plans. Local first responders should be made aware of any doors that require special tools to breach during an emergency.

3.3.5.4 *Concerns About the Technology*

3.3.5.4.1 *What It Does Not Do*

Ballistic tests are generally requested or conducted by manufacturers to determine the bullet resistance of products. Testing for certification is performed with specific procedures that specify the firearm, type of ammunition, distance from the material tested, angle of the shot, and total number of shots. While giving an indication of the level of protection offered by the product, such tests cannot predict how well the product will be able to protect people during an actual incident that may involve more powerful weapons or repeated attempts to breach the material. Therefore, although it seems reasonable that properly installing a bullet-resistant door or panel would provide additional protection against a projectile originating outside the door, additional in-situ testing would be necessary to verify the level of added protection. This testing would ideally ensure projectiles could not be fired through unprotected areas of the door and determine whether projectiles could be deflected by a bullet-resistant panel and subsequently redirected through an unprotected area of the door or frame.

3.3.5.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

As with any safety technology or procedure, it is impossible to predict all scenarios; therefore, even with the best planning a determined intruder may find a way to breach a bullet-resistant door or door covering. If a school cannot strengthen all interior doors at the same time, a school assessment should be conducted and doors in areas with highest risk be strengthened first.

The effectiveness of doors and door coverings relies on a sound structure holding them in place. Schools should consider the overall strength of the doorframes and locking mechanisms. For example, the addition of bullet-resistant coverings will provide limited value if a door can be easily kicked out of its frame or the door handle can be broken off to disengage the lock.

If the entire surface of the door is not bullet resistant, it is important to determine which areas in the room would remain susceptible to penetration by bullets and ensure people do not shelter there.

3.3.5.4.3 *Possibilities for Misuse*

No concerns about misuse were identified for bullet-resistant doors and door coverings.

3.3.5.4.4 *Liability and Safety Concerns*

Door coverings must not prevent locks from engaging or disengaging. Local first responders should be consulted before implementing any technology that could impede their entrance to a room to provide fire or medical assistance.

The method used to attach the bullet-resistant covering to the door is a potential area of weakness. If the covering is on the outside of the door, ensure any screws and attachment frames are tamper proof. If the covering is on the classroom side of the door, it must be secured in such a way that the impact of a projectile passing through the door cannot dislodge the covering.

3.3.5.4.5 *Privacy Concerns*

These physical security options do not involve any collection of personal information.

3.3.5.4.6 *Accommodations Needed for Disabilities*

When installing access control devices or developing emergency procedures regarding their use, school systems must ensure compliance with local, state, and/or Federal fire code and other building and safety regulations, including those related to students with disabilities.

A door covering solution does not change existing doorways or access methods; therefore, it should have no effect on ingress and egress during normal school operations.

3.3.5.4.7 *Other Issues*

As with any product intended to provide protection from projectiles, it is important to verify the independent test results for any claims of bullet resistance. Tests conducted by the manufacturer should not be considered equivalent to certification. Purchasers should consider the manufacturer's warranty as well as the financial viability of the company providing the warranty.

3.3.5.4.8 *Policy Concerns*

Because local fire codes often prohibit modification of fire doors, schools should verify that the doors and installation methods for door coverings meet those fire codes.

3.3.5.5 *Cost Considerations*

The largest cost of adding bullet-resistant coverings to existing doors is the purchase of the door coverings themselves. Prices vary according to the size of the panel, the level of bullet resistance, and additional features such as hinged panels to cover door lights. Vendors may offer standard sizes that are usually less expensive than custom sizes. If multiple doors will use panels of the same size and configuration, there may be a discount for buying in quantity.

Although doors with lower levels of bullet resistance may be priced similarly to door coverings, bullet-resistant doors are usually more expensive, particularly if custom sizes are required for the installation.

There are some additional costs to consider such as labor and installation. There will be labor associated with measuring and recording the sizes for each door ordered, particularly if the door coverings are made to order. Preparing the order and verifying receipt of the correct items will also require labor hours. There may be a need for additional hardware or tools for installation as well as cosmetic parts such as corkboards or dry erase boards to disguise the door covering, and molding, stain, or paint to further incorporate a new door into the existing design. Most doors and coverings are maintenance free and unlikely to have additional upkeep costs.

Generally, installation costs (Table 3-18) will vary depending on whether the door or door covering is installed by the purchaser or by the fabricator. If the number of doors or coverings is significant, it is worth considering whether installation is priced per unit, by labor hours, or for the complete job. Because experience with tools, templates, and installation procedures likely are necessary for installation, it is reasonable to expect the amount of time needed for each installation to decrease after an initial learning curve.

Table 3-18 Bullet-Resistant Doors and Coverings Cost Considerations

Cost Factor	Cost Description
Acquisition	\$500 to \$2300 per bullet-resistant panel, with installation hardware. Bullet-resistant doors range from \$1000 to more than \$50,000 per door (Reference 212), depending on the materials used and the level of resistance.
Installation	Varies based on the solution and existing construction. It may take less than 1 labor hour to install a bullet-resistant panel, but reinforcing ceiling and door structures may be significant factors when adding a heavy bullet-resistant door.
Operation and labor	None
User training	None
Maintenance	Basic cleaning and lubrication for hinges.
Consumables	None
Energy and energy dependency	None
Software licenses	None
System integration	Minimal, may require inspection for fire or building code.

3.3.5.6 Emerging Technologies and Future Considerations

Improvements to the weight of bullet-resistant materials could make this technology easier to implement in existing buildings, whereas advances in production could drop the expense of bullet-resistant doors and coverings, making them more affordable.

3.3.5.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 3-19 provides examples of known vendors of bullet-resistant door coverings; however, it is not comprehensive and other vendors may exist. The list is current as of 10 January 2016.

Table 3-19 Bullet-Resistant Door and Covering Vendors

Vendor	Website	Notes
Assa Abloy	http://www.assaabloy.com/en/com/about-us/products/	doors
Campus Security Systems	http://campussecuritysystems.com/products/door_guard/	coverings
Hardwire Armor Systems	http://www.hardwirellc.com/solutions/school_office/door.htm	coverings
Grainger	http://www.grainger.com	doors
Safer Schools for America	http://www.saferschoolsforamerica.com/	coverings
Steel Door Institute	http://www.steeldoor.org/	doors
Total Security Solutions	http://www.tsbulletproof.com/	doors

For related information, see NIJ's *Active NIJ Standards and Comparative Test Methods*.⁵⁹ It includes standards for bullet-resistant protective materials, body armor, and handheld and walk-through metal detectors.

3.3.6 BULLET-RESISTANT WINDOWS AND FILMS

3.3.6.1 Introduction

Bullet-resistant windows are intended to allow light to enter into the building while protecting the occupants from bullets fired from outside the window. The technology that makes the windows difficult to shoot through also makes them resistant to breakage or forced entry.

For the purpose of this report, several technology-specific terms are associated with this technology:

- **Bullet proof:** Capable of preventing penetration by a bullet fired from a firearm. Because the force of a bullet is highly variable depending on factors such as the type of firearm, type of projectile, and distance from muzzle to target, items meant to be *bullet proof* are best described as *bullet resistant*.
- **Bullet resistant:** Capable of preventing penetration by some types of projectiles, but may allow penetration when subjected to repeated strikes or to higher-powered projectiles. Bullet resistance should be specified in terms of an accepted standard such as NIJ 018.01 or ASTM F-1233 (Nationwide Structures, Inc.)
- **Bullet-resistant glass:** Any transparent material used in windows that allows light to enter a building or room while also offering resistance to gunfire.
- **Bullet-resistant window:** Any window that has increased resistance to gunfire or impact as a result of the use of bullet-resistant glass or the addition of bullet-resistant film.
- **Laminate (noun):** A material composed of two or more layers bonded together.
- **Spall:** May refer to the act of breaking a window into small pieces or the pieces themselves.
- **Window film:** A thin, flexible, transparent material provided as a sheet or roll for application to a window.

3.3.6.2 How the Technology Is Used

Schools generally use glass in their exterior front doors to create an inviting entrance. If the school has physical walls or doors (rather than turnstiles) between the front lobby area and the visitor control area, these also frequently use glass to allow staff to monitor people entering the building. Because these glass windows represent the first defense between the outside and the occupants, enhancing their impact resistance gives people additional time to recognize, escape from, and alert others to an intruder. Following the Sandy Hook Elementary School attack in which the assailant entered the school by shooting out the plate-glass window next to the locked front doors, there has been increased interest in the use of bullet-resistant glass for front entrances.

Windows separating two interior spaces (such as between a hallway and a classroom) are another type of window that may be reinforced. It is uncommon to use bullet-resistant glass in these interior windows unless there is some significant reason to expect an attack; for example, if a school dispenses cash or medications through a specific window, it might make sense to install a bullet-resistant transaction window like that shown in Figure 3-7.

⁵⁹ <http://www.nij.gov/topics/technology/standards-testing/pages/active.aspx>



Source: Transparent Ballistic Solutions

Figure 3-7 Example of a Bullet-Resistant Transaction Window that Allows Conversation and the Passing of Small Items Safely Underneath

By far the most prevalent windows in schools are those that allow occupants to see out of classrooms, offices, and common areas. These exterior windows offer light, which has been shown to have a significant impact on the well-being of students (Reference 23) and may help control interior temperatures. During an emergency, windows can be broken to allow occupants to communicate, add ventilation, or evacuate.

Windows can also be vulnerable to gunfire such as a targeted attack in the case of Sandy Hook, as well as numerous recent reports of bullets striking schools windows without causing injury, for example, in Chicago, IL⁶⁰; Burbank, CA (Reference 385); and Hartford, CT (Reference 232). Reports of people injured by shots fired through an exterior window are less common but do occur, as in the 2009 case of a student struck by a stray bullet while sitting in a classroom in Suffolk County, NY (Reference 347).

3.3.6.3 What Makes the Technology Good?

3.3.6.3.1 How the Technology Works

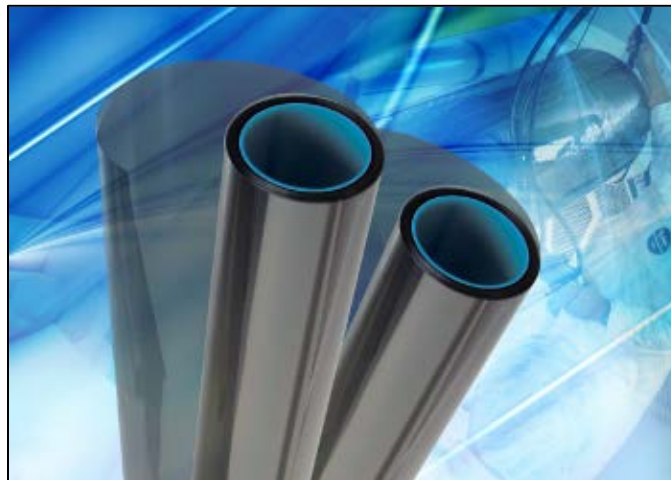
Bullet-resistant “glass” may actually be acrylic or aluminum oxynitride, but most often the term refers to glass-clad polycarbonate, which is composed of transparent polycarbonate plastic sandwiched between layers of normal glass. Glass is actually harder than the plastic; however, it is more rigid and thus more brittle. The plastic layer is flexible and able to absorb the energy of an impact, with the thickness of the plastic determining how much energy it can absorb. For example, a 0.75-inch (19-mm) thick layer of polycarbonate may stop three shots from a 9-mm handgun to provide UL 752 Level 1 protection, but must be 1.25 inches (31.75 mm) thick to reach UL 752 Level 3 protection capable of stopping three

⁶⁰ Eyewitness News 7 – Chicago (2 September 2015) “Circle Rock Charter School Window Hit by Bullet.” Retrieved 9 November 2015 from <http://abc7chicago.com/news/bullet-damages-window-at-west-side-school/967254/>

rounds from a .44 magnum handgun.⁶¹ The hard glass layers protect the plastic from scratches, but also serve to deform bullets, making them flatter and less likely to penetrate the inner plastic layer.

Bullet-resistant film or laminate is a thin layer of plastic (Figure 3-8) intended to add a similar flexible, energy-absorbing layer to existing glass windows. It is applied to standard glass windows, either during window installation or as a retrofit. Window film is usually less than 0.5 inch (12.7 mm) thick and thus absorbs less impact than the thicker plastic layer in glass-clad polycarbonate. Because of this reduced ability to actually stop a bullet, the primary safety function of some thinner bullet-resistant films is the ability to minimize injuries from broken glass and to briefly slow attempts at forced entry. Window film must be properly installed to ensure it provides edge-to-edge protection and does not delaminate from the glass or detach from the frame when stressed.

Regardless of whether made of bullet-resistant glass or enhanced with bullet-resistant film, bullet-resistant windows are intended to absorb the energy from a bullet or strike, delay penetration, and prevent spalling as shown in Figure 3-9.



Source: Johnson Window Films⁶²

Figure 3-8 Window Film Provided on Rolls

⁶¹ Wikipedia (17 September 2015) "Bulletproof glass." Retrieved 9 November 2015 from https://en.wikipedia.org/wiki/Bulletproof_glass

⁶² <http://johnsonwindowfilms.com/all-about-film/>



Figure 3-9 Bullet-Resistant Windows

3.3.6.3.2 Differentiators

The primary consideration for bullet-resistant glass and films is the certified resistance to impact. The vendor should be able to supply the results of independent tests indicating the standard met by the product.

Cost may make it impractical to replace all existing glass windows with bullet-resistant glass.

3.3.6.3.3 Specifications and Features

When considering bullet-resistant windows, their added weight and thickness may be an issue in existing buildings. Building structures must be able to support the weight without allowing the windows to sag, and window frames must allow proper installation of the thicker windows.

When considering a product to increase the bullet resistance of windows, the level of resistance offered by the window or film is an important factor. Several organizations have developed standards used to certify the bullet resistance of materials. Some rating systems, such as the U.S. State Department Standard SD-STD-02.01, European Standard DIN EN 1063, British Standards Institution BS 5052, and German DIN 52-290, specify the bullet-resistant rating by indicating the type of firearm and projectile blocked by the material. The UL 752 and NIJ 018.01 rating systems use a series of numbered levels, where the higher the number, the higher the ability to resist more powerful projectiles. Regardless of the system, all ratings are based on the ammunition type, weight of the projectile, force of the projectile, and number of shots to which the test object is subjected.⁶³ Schools should consult with local law enforcement to understand the types of weapons used in local crimes and in school shootings around the nation to make an informed decision about the level of bullet resistance needed.

⁶³ <http://www.nationwidestructures.com/ballistic-key.html>

3.3.6.3.4 *Effectiveness*

The authors found no reports of attacks against schools with bullet-resistant windows installed; however, if this technology can slow a potential attacker's entry, it may have value in mitigating the effects of an attack.

3.3.6.3.5 *Policy Impacts*

The installation of new windows or window films may require modification to existing emergency plans.

3.3.6.4 *Concerns About the Technology*

3.3.6.4.1 *General Discussion (What It Does Not Do)*

Bullet resistance is tested and certified based on specific weapons and numbers of shots. Even a single shot from a more powerful weapon may pierce the window. Although bullet-resistant glass and film will delay entry, a determined assailant may eventually breach the window. The value of such solutions is to give occupants time to escape or seek cover before the window is breached.

3.3.6.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

If a school is unable to strengthen all windows at the same time, a school assessment should be conducted to determine the areas with highest risk and address those windows first.

Whether using bullet-resistant glass or film, its effectiveness relies on a sound structure holding them in place. Many schools use heating and air conditioning instead of opening windows for temperature control; for bullet-resistant windows to provide protection, they must remain closed. Moreover, if the entire pane separates from the frame or the frame is forced out of the wall as the result of being struck, all protection is lost.

Improper installation may minimize the overall resistance of windows and films. The frames must withstand the weight of heavier bullet-resistant windows and the forces exerted on the glass during an attack. Window film must be embedded into the frame or adhered to the window and the frame to ensure a strong force does not deform and detach it from the frame.

3.3.6.4.3 *Possibilities for Misuse*

No concerns about misuse were identified for bullet-resistant windows and films.

3.3.6.4.4 *Liability and Safety Concerns*

The use of bullet-resistant film on all classroom windows leads to concerns about being able to break the windows for emergency exit. Although repeated blows will breach bullet-resistant glass and film, the effort could be too much for some people, particularly if also subjected to smoke or heat during a fire.

The use of bullet-resistant film inside the school could slow police efforts to reach an intruder who has locked himself into a room. Also, in the unlikely event that law enforcement officers outside the school are able to identify an assailant inside the school and choose to eliminate the threat from outside the school, the use of bullet-resistant window film could impede law enforcement officer ability to apprehend the assailant.

3.3.6.4.5 *Privacy Concerns*

These physical security options do not involve any collection of personal information.

3.3.6.4.6 *Accommodations Needed for Disabilities*

When installing access control devices or developing emergency procedures regarding their use, school systems must ensure compliance with local, state, and/or Federal fire code and other building and safety regulations, including those related to students with disabilities.

A bullet-resistant window solution has no effect on ingress and egress during normal school operations; however, if emergency plans include breaking windows for evacuation or ventilation, the effect on staff and students with disabilities should be addressed.

3.3.6.4.7 *Other Issues*

As with any product intended to provide protection from projectiles, it is important to verify the independent test results for any claims of bullet resistance. Tests conducted by the manufacturer should not be considered equivalent to certification. Purchasers should consider the manufacturer's warranty as well as the financial viability of the company providing the warranty.

3.3.6.4.8 *Policy Concerns*

Schools should confer with local first responders prior to selecting bullet-resistant window options to ensure the windows meet fire codes and that all first responders are aware of the additional force that will be needed to breach the windows.

3.3.6.5 *Cost Considerations*

The largest cost of adding bullet-resistant windows is the purchase of the windows or bullet-resistant film. Prices vary according to the size and number of windows to be protected, the level of bullet resistance, and whether the solution is to install bullet-resistant glass or to fortify existing windows with bullet-resistant film.

The labor associated with measuring windows is generally absorbed by the vendor during the estimation stage. The estimate should also include installation and any modifications to existing construction. Most windows are relatively maintenance free and unlikely to have additional upkeep costs.

Generally, installation costs (Table 3-20) will depend on whether performed by the fabricator or a contractor. In the case of installation of bullet-resistant glass, window frames may need to be modified to accommodate the thicker and heavier glass.

Table 3-20 Bullet-Resistant Windows and Films Cost Considerations

Cost Factor	Cost Description
Acquisition	Varies according to the solution selected, size of each window to be modified, and overall number of windows.
Installation	Varies according to the solution selected and whether installed as part of renovation, retrofit, or new construction.
Operation and labor	None
User training	None
Maintenance	Basic cleaning according to manufacturer's instructions. Note that typical methods used to clean glass windows may scratch window films.
Consumables	None
Energy and energy dependency	May impact building heating and cooling costs if a solar reflective solution is selected.
Software licenses	None
System integration	Minimal, may require inspection for fire or building code.

3.3.6.6 Emerging Technologies and Future Considerations

Advances in bullet-resistant materials could make them more affordable or easier to retrofit to existing buildings. Increased frequency or likelihood of shootings in schools could also drive interest in these products.

3.3.6.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 3-21 provides examples of known vendors of bullet-resistant door coverings; however, it is not comprehensive and other vendors may exist. The list is current as of 10 January 2016.

Table 3-21 Bullet-Resistant Windows and Films Vendors

Vendor	Website	Notes
Bullet Guard	http://www.bulletguard.com/	windows
Grainger	http://www.grainger.com	bullet-resistant materials
Lexgard Laminates	http://www.lexgardlaminates.com/	windows
National Glazing Solutions	http://www.nationalglazingsolutions.com/	films
Total Security Solutions	http://www.tssbulletproof.com/	windows
Westmount Security	http://westmountsecurity.com/shatterproof-your-glass/	films

For related information, see National Glazing Solutions' Safety and Security Window Film Test Results Summary Tool at <https://www.nationalglazingsolutions.com/products/security/>. This online tool allows the user to filter performance test reports by film manufacturer, test scope, and certifying agency. Also

see the *Final Report of the Sandy Hook Advisory Commission*,⁶⁴ which contains recommendations concerning safe school design and operation.

3.3.7 LOCKDOWN DEVICES

3.3.7.1 Introduction

If a threatening person has gained access to the school, one option to prevent the intruder from harming people is to gather students and staff in safe areas and prevent the intruder from entering those areas. In this report, lockdown devices have been divided into two categories based on their intended function. *Anti-latch devices* facilitate the process of securing a room by allowing someone to rapidly engage the existing door lock, whereas *anti-breach devices* prevent the door from being forced open regardless of whether it is locked or not.

For the purpose of this report, the following definitions were used:

- **Lockdown:** Initiated when a dangerous criminal is believed to be inside the building. Generally, lockdown procedures direct occupants of a room to lock themselves in and wait silently until notified that the situation has been resolved.
- **Lockdown device:** A piece of hardware applied to an existing door to facilitate the lockdown process or to prevent the door from being opened by an intruder. Locks and deadbolts integrated into the door and activated using keys or switches are discussed in Subsection 3.3.1.
- **Latch or latch bolt:** The part of a lock that extends out of the door and into the doorframe when the lock is engaged. The design of a latch bolt allows it to be locked while the door is open and then be pushed closed to seat the latch bolt. The door cannot be opened until the latch bolt is disengaged by turning the interior knob to withdraw the latch bolt from the doorframe (as shown in Figure 3-10).
- **Dead bolt:** The part of a lock that extends out of the door and into the doorframe, but when extended while the door is open, it will retract to allow the door to be closed.
- **Strike plate:** A metal plate on the doorframe that the latch bolt passes through when the lock is engaged.

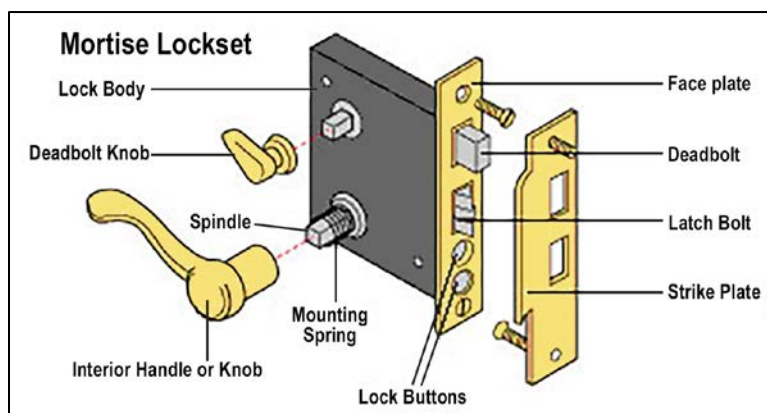


Image copyright Don Vandervort, Hometips.com.

Figure 3-10 Parts of Typical Door Lock Showing Moveable Latch Bolt and Hole in Strike Plate

⁶⁴ http://www.shac.ct.gov/SHAC_Final_Report_3-6-2015.pdf.

3.3.7.2 How the Technology Is Used

Some schools keep classroom doors locked during instruction periods to ensure students are protected from intruders without the need to specifically identify a threat and initiate a lockdown. Many schools prefer to keep classroom doors unlocked during instruction periods to allow students to take restroom breaks without requiring someone to let them back in and to ensure another staff member can enter easily, if needed. During a lockdown, the teacher must physically lock the classroom door. However, there are concerns that during the stress of an emergency, teachers might have difficulty with the fine motor skill needed to fit the key into the lock. There is also the risk that a key will be unavailable when needed.

3.3.7.2.1 *Anti-latch Devices*

One compromise is to have the door locked at all times but prevent the lock from engaging until needed. Anti-latch devices prevent the latch bolt from seating into the doorframe. Thus, the door is “locked” and yet it can be opened and closed without turning the handle. When it is necessary to allow the door to lock, the obstruction is removed and the already locked latch bolt extends and engages as soon as the door is shut.

3.3.7.2.2 *Anti-breach Devices*

Some schools do not have locks on classroom doors, or there is concern that an intruder could force a locked door to open. Anti-breach devices make it difficult for an attacker to open the door, regardless of whether it is locked or not. The device is generally stored near the door until needed, at which time it must be moved into position to engage the device.

3.3.7.3 What Makes the Technology Good

3.3.7.3.1 *How the Technology Works*

3.3.7.3.1.1 *Anti-latch Devices*

Anti-latch lockdown options prevent the door latch from fully engaging by blocking the opening into which the latch seats, by causing the door to remain slightly ajar, or by keeping the door handle in the unlocked position. Figure 3-11 presents examples of anti-latch devices.

When a door handle is turned, it retracts the latch bolt, like the one shown in Figure 3-10, from the hole in the doorframe and allows the door to open. The design of a latch bolt allows it to be locked while the door is open, and then pushed closed to seat the latch bolt. The locked door can be opened easily from the inside by turning the knob to withdraw the latch bolt from the doorframe, but is locked from the outside.



Sources: Clockwise from top right: InslideLockdown, Global Innovations School Safe, Classroom Secure Rapid Lock System, and Lockdown Magnet.

Figure 3-11 Examples of Anti-Latch Devices

3.3.7.3.2 Anti-Breach Devices

The anti-breach products identified for this report operate using one of three basic principles: they use friction to prevent the door from being pushed open; they prevent the arms of a hydraulic unit from opening; or they temporarily attach the door to floor, doorframe, or wall.

Options for inward-opening doors include forcing the back of a chair under the door handle or using desks and chairs to barricade the door, thus making it harder to open because the intruder must use enough force to move the additional objects. This method requires people to place themselves near the door and thus closer to a potential threat while constructing the barricade. It is also likely to make noise that could alert an intruder to the location of possible targets. Such a barricade does not help with outward-opening doors. A variety of devices exist to help prevent inward- and outward-opening doors from being forced open.

Security bars (Figure 3-12) rely on the same concept as jamming a chair under the door handle of an inward-opening door, but they are designed to be height adjustable and have feet designed to avoid slipping on a variety of floor surfaces. Security bars must be stored near the door until needed, and then they must be properly positioned during lockdown to be effective. They can be overcome if sufficient force is applied to either bend or break the bar, if the bar can be dislodged from the door handle, or if the foot slides across the floor.



Source: Fighting Chance Solutions⁶⁵

Figure 3-12 Example of Security Bar Installed To Form a Brace Between Door Knob and Floor, which Inhibits Opening the Door Inward

Doors with hydraulic closers can be prevented from opening by securing the scissoring arms of the door with straps or a sleeve of metal or plastic (Figure 3-13). These options require that someone can reach to the top of the door, which may be difficult for shorter people, children, and people with disabilities or injuries.

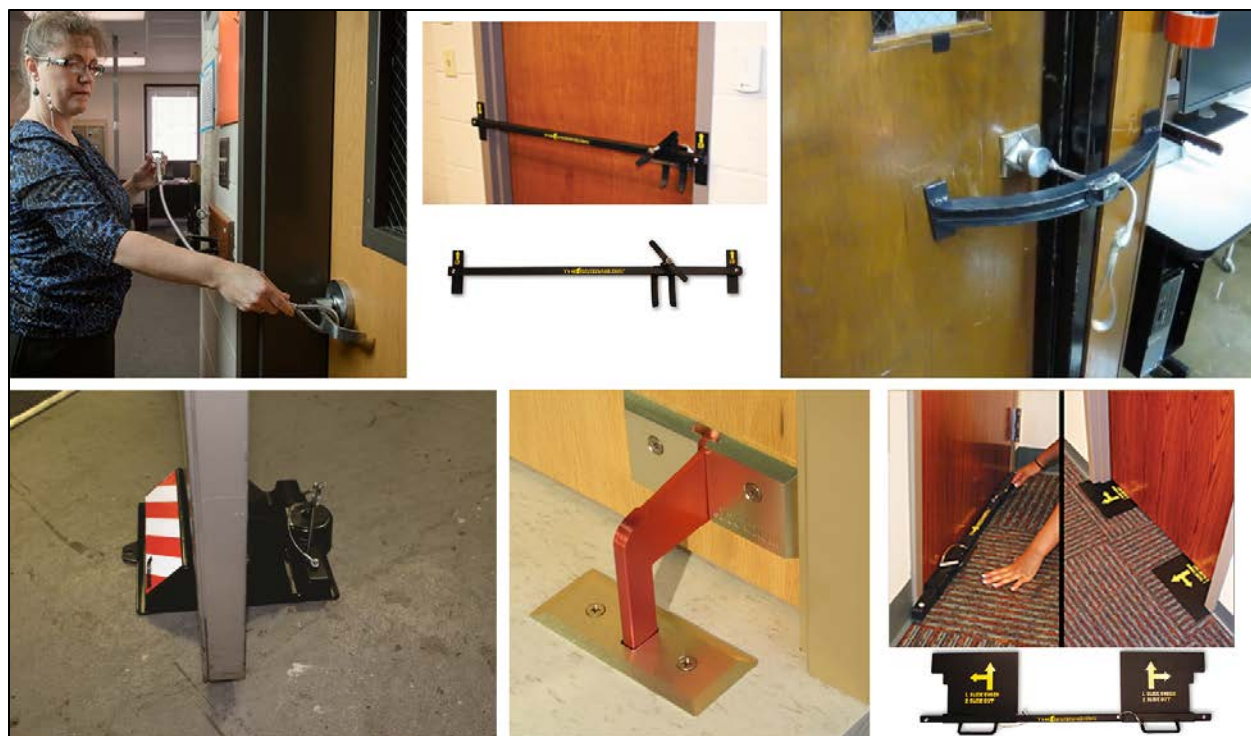


Sources: Fighting Chance Solutions and Hydra-Lock

Figure 3-13 Examples of Metal Sleeve and Strap Options to Prevent a Hydraulic Door from Opening

The most common type of anti-breach devices found during the research for this study function by attaching a physical device to both the door and an anchor point in the floor, doorframe, or wall. Several forms are shown and described in Figure 3-14.

⁶⁵ <http://fightingchancesolutions.com/shop/rampart/>



Clockwise from top left: PALS attaches the doorknob to a wall anchor using a steel cable, whereas Barracuda DCO and Lockemout use metal bars to connect the doorknob to the doorframe. Bearcade and Night Lock use a door stop attached to the floor, whereas Barracuda DCI uses a brace that grips the doorframe to prevent the door from opening.

Figure 3-14 Examples of Anti-Breach Devices that Anchor Door to Surrounding Structure

3.3.7.3.3 Differentiators

The selection of a lockdown device will be based on a variety of factors. Schools should first consider whether the primary goals are process related, such as the need to make the lockdown process easier for teachers, to ensure teachers can lockdown without opening classroom doors, to prevent failure due to missing keys, or to find a solution that allows administrators or police to unlock the doors from the hallway.

Cost of purchase and installation may be critical, but the strength, type, and materials of existing doors and locks are more likely to determine what devices will be effective. Some devices work on doors that open outward, whereas others require an inward-opening door.

Applicable laws may prohibit some devices, such as jurisdictions that do not allow screws to be driven into fire doors.

3.3.7.3.4 Specifications and Features

After determining the goals of the lockdown device and identifying the types of doors and locks in the school, schools can begin to select from a variety of devices available. Table 3-22 shows a representative sample of lockdown devices available when this study was conducted.

Table 3-22 Comparison of Features of Various Types of Lockdown Devices

Examples of Devices			Secures Door Types			Must Modify		Lockdown Activation				Other
Anti-	Format	Product	Open Out	Open In	Double Doors	Door or Frame	Floor, Wall, or Ceiling	Works without Locking Door	Engages without Opening Door	Unit is Always Installed	Police can Override	Notes
Breach	Floor pin	Bearacade	Y	Y	Y	N	Y	Y	N	N	N	Requires reaching the floor
Breach	Floor pin	Bearacade B2	N	Y	?	N	Y	Y	Y	N	N	Requires reaching the floor
Breach	Block scissor	the Sleeve	Y	N/A	?	N	N	Y	Y	N	N	Requires reaching top of door
Breach	Security bar	the Rampart	N	Y	?	N	N	Y	Y	N	N	–
Latch	Prevent closure	School Safe	Y	Y	Y	N	N	N	Y	Y	Y	–
Latch	Block latch	InSlide Lockdown	Y	Y	?	Y	N	N	Y	Y	Y	–
Breach	Block scissor	Barracuda DCS	Y	N/A	?	N	N	Y	Y	N	N	Requires reaching top of door
Breach	Door brace	Barracuda DSO	Y	N/A	?	N	N	Y	Y	N	N?	–
Breach	Floor pin	Barracuda DSI	N	Y	?	N	N	Y	Y	N	N?	Requires reaching the floor
Breach	Door brace	NightLock	Y	Y	Y	Y	Y	Y	Y	N	Y	Requires reaching the floor
Breach	Door brace	the Boot	Y	Y	Y	Y	Y	Y	Y	N	Y	–
Latch	Block handle	Rapid Lock System	Y	Y	?	N	N	N	Y	Y	Y	Requires lever handle, not door knob or push bar
Latch	Block latch	Door Blok	Y	Y	?	N	N	N	N	Y*	Y	Easily removed
Latch	Prevent closure	Lock Blok	Y	Y	?	N	N	N	Y	Y	Y	–
Latch	Block latch	Lockdown Magnets	Y	Y	?	N	N	N	Y	Y	Y	Requires steel doorframe
Breach	Door brace	PALS	Y	Y	?	N	Y	Y	Y	N	N	–
Breach	Block scissor	Hydra-Lock	Y	N/A	?	N	N	Y	Y	N	N	Requires reaching top of door

3.3.7.3.5 *Effectiveness*

The authors were unable to find cases where lockdown devices were used in an emergency situation. Schools should contact manufacturers of specific products to determine whether any testing or certification has been conducted.

3.3.7.3.6 *Policy Impacts*

The effects of these devices on internal policies related to locking doors during school hours and emergency response procedures should be evaluated before a selection is made. See Subsection 3.3.7.4.8 regarding external policies that may impact selection of lockdown devices.

3.3.7.4 *Concerns About the Technology*

3.3.7.4.1 *General Discussion (What It Does Not Do)*

If a lockdown is not initiated and the device engaged before an intruder reaches the door, no benefit will be derived from the device. This may be caused by a failure in the lockdown notification process or a person being unable to locate or properly engage the lockdown device. In addition, any lockdown device is ultimately only as strong as the door it reinforces. Anti-latch devices offer no additional protection. If the door or doorframe can be broken, an anti-breach device can be overcome.

3.3.7.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

Anti-latch devices rely on the door being locked at all times. Disengaging the anti-latch device and pulling the door shut will fail if the door is in an unlocked state and the person initiating lockdown does not notice.

Anti-breach devices with weak components may fail despite being constructed of otherwise strong materials. For example, if a device functions by preventing the hydraulic hinge from opening, but sufficient force on the door can cause the hinge to separate from the door, the overall protective effect would be lost.

Anti-breach devices must be properly positioned and operated during lockdown. Some devices require opening the classroom door to place the device, being able to reach the top of the door or the floor, being able to lift and hold the device while engaging moving parts, or being able to align pins with holes in the floor or wall. These actions may be difficult to perform under stress. There is a risk of being unable to locate or quickly retrieve a device that is not conveniently stored. Any device that is easily portable or uses a separate locking pin offers the possibility of the necessary part being out of reach when needed.

All lockdown devices should allow people to quickly disengage them without tools or training to escape from the room, if necessary.

3.3.7.4.3 *Possibilities for Misuse*

Lockdown devices not permanently attached are subject to being stolen or misplaced. A student or staff member who intends to cause harm could remove the device from an intended target location. Keys or tools intended to allow first responders to disengage lockdown devices from outside the classroom could also be stolen by someone with access to the school before an attack.

Some school security experts believe the risk that someone could use a lockdown device to lock a victim into a room to commit a crime, such as a sexual assault, outweighs their value against a school shooter (Reference 339). However, this concern would also apply to classroom doors with locks.

3.3.7.4.4 Liability and Safety Concerns

Schools should verify device compliance with local, state, or Federal laws before purchasing lockdown devices. For example, Ohio schools that have already purchased lockdown devices may be affected by the State Standards Board's recent conclusion that lockdown devices must allow doors to be easily opened from the inside of a classroom without a key or special knowledge; they must not require tight grasping, pinching, or twisting of wrists to operate; and unlatching a door cannot require more than one operation. Schools have been advised against purchasing additional lockdown devices until the board finalizes rules about acceptable use (Reference 65).

3.3.7.4.5 Privacy Concerns

No privacy concerns related to the use of lockdown devices were identified by the authors.

3.3.7.4.6 Accommodations Needed for Disabilities

When installing access control devices or developing emergency procedures regarding their use, school systems must ensure compliance with local, state, and/or Federal fire code and other building and safety regulations, including those related to students with disabilities

Although it is important to ensure all teachers can engage lockdown devices in an emergency, students and visitors may also need to secure classroom doors. Devices usable only by a subset of the school population should be considered with caution. A recent legal decision in Ohio banned the use of lockdown barriers until policies can be defined because of concerns that the hand motions required to use them and the locations the user must be able to reach (for example the floor) may violate Federal disability laws (Reference 339).

3.3.7.4.7 Other Issues

All of the lockdown devices identified during research for this study are constructed of relatively simple hardware without motors, electronics, or software. The market contains numerous products invented by concerned individuals who designed a device and then distributed the devices to local schools. Schools should carefully check that any lockdown device is properly patented or licensed, has been independently tested for effectiveness, and is backed by a manufacturer or distributor that can provide follow-up service as needed.

3.3.7.4.8 Policy Concerns

Any lockdown device that requires modifying a fire door or disrupting its normal operation should be discussed with the local fire department to ensure compliance with fire codes. Codes may also prohibit any device that prevents first responders from being able to enter a classroom without the assistance of someone inside the room to disengage the lockdown device. Devices could violate the Americans with Disabilities Act if they cannot be operated by everyone in the building. Additionally, the effects of these devices on internal policies related to locking doors during school hours and emergency response procedures should be evaluated before a selection is made.

3.3.7.5 Cost Considerations

The purchase price for these devices varies, but generally ranges from approximately \$3.25 to \$150. The initial purchase price is not the only cost consideration in schools (see Table 3-23).

Table 3-23 Lockdown Device Cost Considerations

Cost Factor	Cost Description
Acquisition	Devices ranged from \$3.25 for a lockdown magnet to \$150 for steel door braces. Many vendors offer volume discounts.
Installation	Varies. There will be installation labor costs associated with devices that are permanently attached; that require modifications to doors, floors, or walls; and/or that require a separate storage component. Installation fees may be a significant part of the overall cost. As an example, vendor installation of a \$50 NightLock device, which requires drilling into the door and floor, quotes installation fees of \$40 per unit.
Operation and labor	None
User training	Varies. The more steps involved and the more precise the placement must be to ensure proper operation, the more critical training and periodic drills will be.
Maintenance	None noted, but some devices may require routine cleaning, lubrication, or inspection. Devices that require sliding a locking pin into holes in classroom floors or doorframes may require special cleaning to ensure the holes are free of debris.
Consumables	None
Energy and energy dependency	None
Software licenses	None
System integration	None

3.3.7.6 Emerging Technologies and Future Considerations

Policy reviews by various local and state regulatory agencies are likely to have a significant impact on the acceptance of these devices.

3.3.7.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 3-24 provides example of known vendors of lockdown devices; however, it is not comprehensive and other vendors exist. The list is current as of 10 January 2016.

Table 3-24 Lockdown Device Vendors

Vendor	Website	Notes
Bilco	http://www.bilco.com/Barracuda-Intruder-Defense-System.html	Anti-breach devices
Bearacade	http://doorbearacade.com	Anti-breach devices
Door Blok	http://www.doorblok.com	Anti-latch device
Classroom Secure	http://www.classroomsecure.com/	Anti-latch device
Fighting Chance Solutions	http://fightingchancesolutions.com	Anti-breach devices

Table 3-24 Lockdown Device Vendors (Continued)

Vendor	Website	Notes
Global Innovations	http://globalinnovationsco.com/	Anti-latch devices
Inslide Lockdown	http://www.inslidelockdown.com/	Anti-latch devices
Intruder Response	http://intruderresponse.com/product-category/lockdown-devices	Anti-breach devices
Lockdown Company	http://thelockdownco.us/the-boot/	Anti-breach device
Lockdown Magnet	http://www.lockdownmagnet.com/	Anti-latch device
Lockdown Solutions	http://www.lockdownsolutions.org	Anti-breach device
Lockemout	https://www.lockemout.com/	Anti-breach device
NightLock	http://nightlock.com/classroom-lockdown/	Anti-breach device
Qwicklock	http://www.qwicklock.com	Anti-breach device

3.4 IDENTIFICATION CARDS

3.4.1 INTRODUCTION

The type of system discussed in this section aims to control school access by ensuring individuals on school campuses are easily identified and visitors are distinguishable from students, faculty, and staff. It also aims to easily manage access to specific locations, facilities, and/or functions.

The need to easily identify individuals on school property is not a new concept in school security or access control. As noted by the National Crime Prevention Council,

*The Southeast Regional Vision for Education’s 1993 report, Reducing School Violence: Hot Topics and Usable Research, recommends students and staff ID cards as one of many successful strategies for ‘keeping unauthorized persons off campus’ and ensuring the safety and security of students and staff. [Additionally], according to a 1993 study by the National School Boards Association, 32 percent of all school districts surveyed reported successful use of student and staff photo ID card systems. The rate of use was 41 percent in urban school systems. The report highlights seven districts in six states that use the systems with success.*⁶⁶

3.4.2 HOW THE TECHNOLOGY IS USED

ID cards can serve as means of ID by associating an individual with information that can verify (visually or otherwise) identify, affiliation, access permissions, etc. Advancements in technology have resulted in increased technologies associated with ID cards. For example, ID and smart card vendor AlphaCard notes that “an employee ID card can also serve as an electronic door key, a time and attendance card, or even a cashless payment card at the school cafeteria. By integrating more than one use for ID badges, [schools] can both streamline operations and increase security.”⁶⁷

⁶⁶ <http://www.ncpc.org/topics/school-safety/strategies/strategy-student-faculty-staff-and-visitor-id-cards>

⁶⁷ <http://www.alphacard.com/learning-center/ways-to-use-your-id-cards/multifunctional-plastic-cards>

3.4.3 WHAT MAKES THE TECHNOLOGY GOOD?

3.4.3.1 How the Technology Works

Electronic “smart” ID cards are encoded with data (of varying amounts depending on the particular function or system chosen). Examples of smart card encoding technologies include

- Barcodes
- Magnetic strip encoding
- Proximity cards
- Contact cards
- Contactless cards
- RFID chips⁶⁸

When used for access control purposes (electronic lock systems), “The [ID] card is swiped or waved in front of [a] reader, which processes and verifies the information on the card before allowing access. This process is more secure than keyed entry because if an [ID] card is ever lost, or makes its way into the wrong hands, it can simply be deactivated. It’s also virtually impossible to duplicate the cards, unlike standard keys.”⁶⁹

3.4.3.2 Differentiators

In addition to serving as electronic keys, smart ID cards and their associated software systems can grant or restrict access to card holders (in some cases, in real time), provide alerts for ID suspensions and invalid IDs, acknowledge and silence door alarms, and facilitate other custom criteria.

3.4.3.3 Specifications and Features

Electronic access control systems require power and, in some cases, either hardwired or wireless networking. Most electronic locking units are powered via hardwired battery, but other options are available. Additionally, mobile scanning units (for functions not associated with specific locks) are available. As mentioned in an *Education Week* article in January 2010 (Reference 13), “Hand-held card scanners are becoming increasingly popular, says [Andrea Wilkins, the national sales manager for the K-12 market for Plasco ID, a Miami-based company that sells and installs ID products]. Administrators can now carry the scanners with them through the hallways when students are supposed to be in class and pull up information such as a student’s schedule—on any stragglers. Mobile scanners can also be taken on field trips to help keep track of students, she says.

As previously discussed, ID cards have the potential to serve a number of purposes in a school setting. There are several factors to consider when implementing or upgrading ID card or badge systems:

- **Desired functionality:** ID cards can range from simple means of ID using printed names, pictures, and/or codes [via card (carried) or badge (worn)] to more complex electronic devices with proximity sensors, RFID capabilities, and other non-access-control-related functions.
- **Location:** The physical locations to place swipe, RFID, or proximity sensors include doors, checkout lanes, turnstiles, etc. Consider all possible locations, and if installing locks with

⁶⁸ <http://www.alphacard.com/learning-center/ways-to-use-your-id-cards/multifunctional-plastic-cards>

⁶⁹ <http://www.alphacard.com/learning-center/ways-to-use-your-id-cards/access-control>

associated electronic or smart ID cards is not feasible, consider the following recommendation from the NCEF (Reference 240):

Electronic controls are not needed at every door but can be used selectively (especially to keep costs down.) If a facility's outer doors are secured electronically, internal areas might be secured with conventional locks. Electronic locks may be worth considering for doors that provide access to higher security areas as well, or for areas that a school would prefer not to have to supervise. For example, if the parking on the west side of the building is for staff only, the west side door can be unsupervised, allowing entry only to those who carry access cards.

- **ID card population:** Consider which populations will be required to carry and/or wear an ID card, such as all teachers and staff, only visitors, or anyone who accesses the school including students. Consider whether the populations will need different types or levels of access and/or if the ID cards and badges can be designed in such a way as to easily distinguish different population groups. Also identify how to handle temporary (visitor) vs. permanent (teacher or student) cards and which access levels are appropriate to each population.
- **ID card policy and guidance:** Once functionality, population, and locations have been determined, it is important to develop clear (and concise) policies and guidance for the use of ID cards. Policies and guidance should address items such as who needs an ID card or badge and how to obtain one, how to distinguish between different ID cards and badges, what to do if an individual sees someone without an ID card or badge, what to do if an ID card or badge is lost or found, etc.
- **Coordination with visitor management systems:** Simple ID cards are independent forms of ID, but newer electronic cards have the capability to be tied into software systems for specific functional uses or more broadly into visitor management systems. Consider how independent or connected the ID card system(s) in the school should be.

3.4.3.4 Effectiveness

According to a 2015 article in *Security Today* (Reference 191) on the use of ID cards in schools, “survey results confirm the top three uses for ID badges are building and facility access, visual identity, and lunch programs.” To implement an effective ID card program for any one or all of these purposes, the ID cards themselves should be hard to duplicate or tamper with (with many schools using “holographic overlays and other security features”) while also potentially considering other factors such as “ease of use, nonacademic uses, and display of school pride.” (Reference 118) ID cards such as these (that are harder to replicate) paired with known and practiced ID card use policies ensure the greatest likelihood for effectiveness in preventing and deterring unauthorized access and other activities.

3.4.3.5 Policy Impacts

An additional point of consideration when installing access control devices or developing emergency procedures regarding their use is to ensure compliance with local, state, and/or Federal fire code and other building and safety regulations including those related to students with disabilities. Because ID cards may impact the process for entering and exiting a school (e.g., a student may have to show an ID to enter the school or access a particular part of the school), general access control policies should be reviewed and evaluated to be consistent with any new ID card function and use (e.g., ID cards that function as electronic keys).

3.4.4 CONCERNS ABOUT THE TECHNOLOGY

3.4.4.1 General Discussion (What It Does Not Do)

ID cards cannot physically prevent an intruder from bypassing the ID system. This technology must be combined with physical barriers such as turnstiles and locks.

3.4.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Individual ID cards are vulnerable to counterfeiting; therefore, staff or any individual responsible for visually inspecting ID cards and granting access should be trained to identify falsified cards. Additionally, electronic cards are vulnerable to electronic manipulation (e.g., changing access permissions) that may or may not render the ID card inoperable. Because these systems can be manipulated electronically in mass, particularly through system software, anti-virus and other defense measures should be in place or provided by the vendor.

3.4.4.3 Possibilities for Misuse

The most common misuse of ID cards is when an authorized person uses a card to grant someone else access. While this may intended as a harmless case of helping someone who forgot their card, it can also be used to allow someone onto the property who should not be there, or with electronic card readers it can be a way to prevent the system from accurately recording who is on the property.

3.4.4.4 Liability and Safety Concerns

No immediate liability or safety concerns were identified.

3.4.4.5 Privacy Concerns

Because many ID cards, especially smart ID cards, contain personal data (such as name, staff ranking, school affiliation, account information, address), a major concern when using them is data protection. As noted by the NCEF (Reference 240), “Whether devices are free-standing or tied into a central processor, if they are too accessible they may be vulnerable to technologically savvy intruders. As a precaution, it may be wise to install lock activation devices or relays on the secured side of the installation, in line with the conventional security panel approach.”

It is also recommended that schools keep only the minimal amount of data necessary to accomplish its ID and access control functions and that they create and implement a plan for removing or deleting that data when it is no longer needed.

3.4.4.6 Accommodations Needed for Disabilities

When installing access control devices or developing emergency procedures regarding their use, school systems must ensure compliance with local, state, and/or Federal fire code and other building and safety regulations, including those related to students with disabilities.

The effects on ingress and egress by people with disabilities should be considered prior to selecting this technology.

3.4.4.7 Other Issues

No additional issues were identified by the authors.

3.4.4.8 Policy Concerns

The primary policy concerns associated with ID cards are the privacy issues discussed in Subsection 3.4.4.5. In addition, if accountability of staff, teachers, and students is a concern in an emergency, administrators should identify what, if any, role ID cards and/or ID card readers play in evacuation procedures.

3.4.5 COST CONSIDERATIONS

ID cards and their associated software and hardware can vary in price depending on several factors. In addition to the initial purchase, which includes individual card readers, ID cards, and software, other costs to consider are discussed in Table 3-25.

Table 3-25 ID Card Cost Considerations

Cost Factor	Cost Description
Acquisition	Acquisition cost can vary depending on the type and features of the ID card system purchased. Traditional ID cards without any electronic access capability are less expensive than integrated ID and door lock systems.
Installation	Installation cost will vary depending on the number and types of units purchased. In the case of electronic door locking systems, some retrofitting or other modifications to account for battery or other power may be needed.
Operation and labor	To issue, replace, remove or destroy, and control access levels for ID cards, administrative staff is required. Competent administration of the system is key for ensuring these types of access control systems keep accurate and timely data.
User training	As discussed, policies and guidance on the use of ID cards and their systems are key for the effective use of these systems in schools. Implementation of these policies and guidance requires training for students, teachers, and other school staff to ensure they are comprehensive (training allows for the identification of gaps) and well-known.
Maintenance	Maintaining hardware and software components to the ID system(s) is critical to ensure the ID cards are functioning properly. This may include periodic purchases of software licenses, replacing batteries, purchasing parts for and servicing ID card printers, etc. Additionally, maintaining an operating system requires accounting for power and network redundancies.
Consumables	ID cards themselves are known consumables for these systems, and the rate of consumption depends on policies about who the cards are issued to and when they are renewed, returned, etc.
Energy and energy dependency	ID card systems used as access control devices (card readers) and as point of sale systems, etc., require energy use and consumption (often in the form of batteries).
Software licenses	Depending on the system and vendor used for electronic ID systems, software license cost will be a factor. License agreements will vary depending on the length and terms of the license and are usually vendor-specific.
System integration	Electronically equipped ID cards can be integrated with a number of access control systems including door locks and turnstiles. Additionally they can be used for non-security purposes such as sales and purchases, library rentals, etc.

3.4.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

As discussed in Subsection 3.3.1.6, electronic access control systems are becoming increasingly sophisticated. Biometric locks and readers are an emerging technology which schools may consider adding to their access control systems. Whether integrated into a locking mechanism or used solely for identity verification purposes, biometric readers are available in a variety of types including fingerprint, iris, and facial scanners. Fingerprint scanning devices are relatively well developed, but they and other biometric devices require a known library of biometric scans (of known fingerprints) to identify individuals. Fingerprinting all possible individuals who might need access and maintaining accurate databases may produce an administrative burden. Additionally, these systems can, like traditional hardware locks, be vulnerable to attack. When paired with electronic ID and access cards, these systems can provide multi-factor authentication, making them more difficult to bypass surreptitiously.

3.4.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 3-26 provides examples of known vendors of ID cards; however, it is not comprehensive and other vendors may exist. The list is current as of 10 January 2016.

Table 3-26 ID Card Vendors

Vendor	Website
AlphaCard	http://www.alphacard.com/
HID Global (Assa Abloy)	http://www.hidglobal.com/
Identicard	http://www.identicard.com/
Identification Systems Group	http://www.identificationsystemsgroup.com/
Plasco ID	http://www.plascoid.com

3.5 CONCLUSION

This chapter covers a broad range of access control devices that are all aimed at preventing or otherwise controlling physical access to school property, people, and/or resources. Some of these systems impact a wide variety of school infrastructure and applications (e.g., locks and fencing), whereas others are for more specific use cases (e.g., bullet-resistant windows). School officials should carefully consider the capabilities, limitations, costs, policy impacts, and other relevant factors prior to upgrading or installing access control systems. Systems available in many of the access control categories discussed are being continually improved as available and/or applicable technologies advance (e.g., biometric reader lock capabilities). School officials should carefully consider the potential technological advancement of these systems and, when possible, accommodate current and future system integration and upgrade possibilities. Many of the technologies discussed can be integrated with access control or other systems (e.g., surveillance systems and cameras) to provide more robust school safety capabilities.

Chapter 4. TECHNOLOGY REVIEW – ALARMS AND SENSORS

Patrick A. Shilts, MS

4.1 INTRODUCTION

Alarms and sensors, a collective system of components that operate autonomously to enable the early detection of intruders, are discussed as they relate to violent crime prevention and detection in schools. They are particularly useful in quickly engaging school and law enforcement officials. Sensors discussed in this chapter include motion sensors such as passive infrared (PIR), microwave motion sensor, and ultrasonic; photoelectric beam sensors such as through-beam, retro-reflective, and diffuse-reflective; and open-door sensors such as magnetic and contact. Alarms covered in this section include panic buttons, badge alarms, silent alarms, and alarm panels.

Figure 4-1 depicts an overall view of how alarms and sensors integrate with each other and how law enforcement, school officials, school visitors, and intruders may interact with each component.

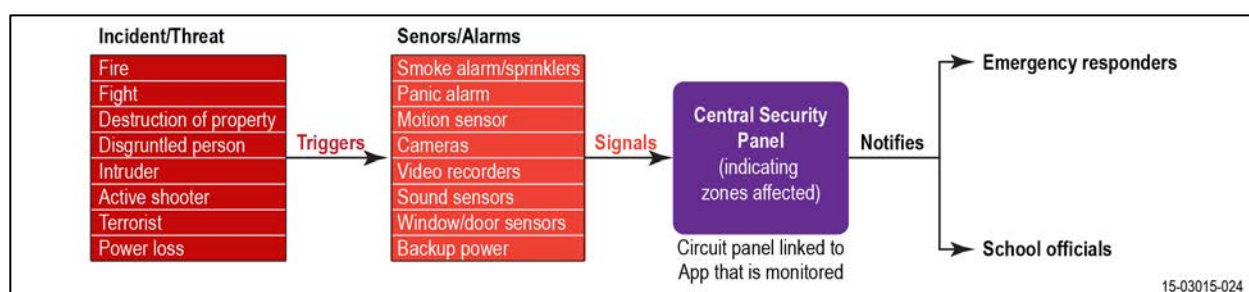


Figure 4-1 Sensors and Alarms Integration with School Stakeholders

The alarm panel serves as the central component and connects the other components, and is also the primary device that school officials use to control the other devices. Motion sensors connect directly to the alarm panel and do not necessarily require human intervention to detect an intruder. Although alarms also connect directly to the alarm panel, they require human action to trigger.

It is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district prior to purchasing a safety or security technology. Table 4-1 presents the means by which the study team evaluated alarms and sensors capabilities, aligned with the Federal Emergency Management Agency (FEMA) mission areas: Prevention, Protection, Mitigation, Response and Recovery.¹ This assessment combines the opinion of security subject matter experts and the informed judgment of the authors who evaluated the technologies. Reviewing this table provides a summary of the areas of school security and safety for which alarms and sensors may be best suited.

Table 4-1 Alarms and Sensors – Technology Impact Summary

Alarm or Sensor	Prevent	Protect	Mitigate	Respond	Recover
Intrusion and Access Sensors					
Motion sensor	LOW Enables detection of intruders typically when school is unoccupied	NONE Does not physically intervene to protect victims from an incident	NONE No effect to mitigate impact was noted	NONE No effect on response was noted	NONE No effect on recovery was noted
Photoelectric beam sensor	LOW Enables detection of intruders typically when school is unoccupied	NONE Does not physically intervene to protect victims of incident	NONE No effect to mitigate impact was noted	NONE No effect on response was noted	NONE No effect on recovery was noted

¹ The preparedness cycle consists of the following five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.
- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

Table 4-1 Alarms and Sensors – Technology Impact Summary (Continued)

Alarm or Sensor	Prevent	Protect	Mitigate	Respond	Recover
Open-door sensor	MEDIUM Enables detection of open doors	NONE Does not physically intervene to protect victims of incident	NONE No effect to mitigate impact was noted	NONE No effect on response was noted	NONE No effect on recovery was noted
Duress Alarms					
Panic button	LOW Provides school officials the ability to quickly trigger an alarm if an intruder is seen	LOW Does not physically intervene to protect victims of incident	MEDIUM May trigger lockdown or emergency response	MEDIUM May shorten the time required to notify first responders	NONE No effect on recovery was noted
Badge alarm	LOW Enables early detection of intruders	LOW Does not physically intervene to protect victims of incident	MEDIUM May trigger lockdown or emergency response	MEDIUM May shorten the time required to notify first responders and identify specific location of badge wearer	NONE No effect on recovery was noted
Silent alarm	LOW Enables early detection of intruders	LOW Does not physically intervene to protect victims of incident	MEDIUM May trigger lockdown or emergency response	MEDIUM May shorten the time required to notify first responders	NONE No effect on recovery was noted
<p>Impacts as they relate to a technology's ability to impact a school's ability to <i>prevent, protect, mitigate, respond, or recover</i> from an incident.</p> <p>High: Technology is expected to have a <i>significant</i> impact.</p> <p>Medium: Technology is expected to have <i>some</i> impact.</p> <p>Low: Technology is expected to have <i>little</i> impact.</p> <p>None: Technology is expected to have <i>no</i> impact.</p> <p>Caution: Technology will have an impact; however, it may also have unintended consequences.</p>					

Further details about each of these alarm and sensor system types are provided in Sections 4.3 and 4.4.

4.2 UTILIZATION STATISTICS

The research team did not find comprehensive statistics on use of alarms and sensors and their impact on school safety.

4.3 INTRUSION AND ACCESS SENSORS




A sensor is “a device that responds to a physical stimulus (e.g., heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse as a measurement or operating a control.”² For school security, sensors are used to automate the detection of intruders by actively monitoring various conditions of the school environment. Sensors commonly used in schools include motion sensors, photoelectric beam sensors, and open-door sensors.

4.3.1 MOTION SENSORS

4.3.1.1 Introduction

“A motion sensor is a device that detects physical movement on a device or within an environment.”³ Common motion sensors can leverage multiple technology types to optimize motion detection. The types of motion sensor technologies discussed in this chapter are displayed in Table 4-2.

Table 4-2 Examples of Motion Sensors

Motion Sensor Type	Description	Example
Passive Infrared (PIR)	Detects movement by sensing changes in thermal energy. When the sensor detects changes in the thermal energy in a room (due to a moving person/object), it triggers an alarm.	 4
Microwave	Detects movement using electromagnetic energy waves. When the sensor detects changes to the electromagnetic energy waves (caused by a moving person/object), it triggers the alarm.	 5
Ultrasonic	Detects movement of an object using acoustic sound waves. When the sensor detects changes to the acoustic sound waves (caused by a moving person/object), it triggers the alarm.	 6

² <http://www.merriam-webster.com/dictionary/sensor>

³ <https://www.techopedia.com/definition/30233/motion-sensor>

⁴ <http://www.bootic.com/ge/home-and-garden/home-security/ge-nx-481-indoor-saw-passive-infrared-motion-sensor>

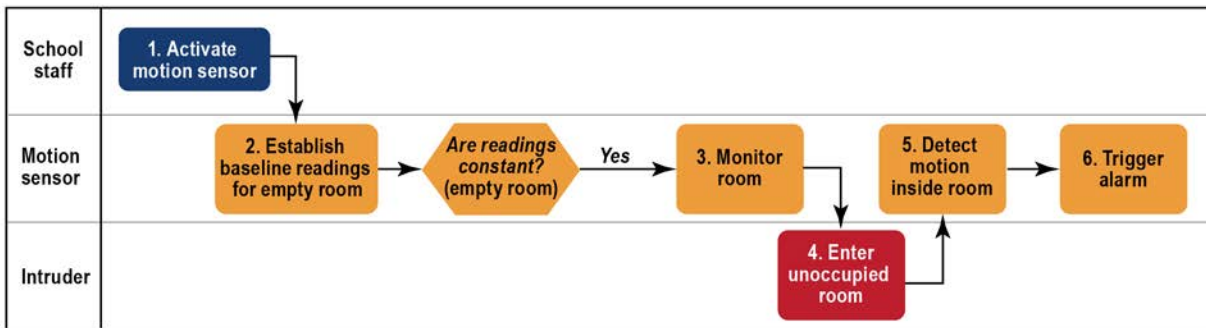
⁵ <http://www.globalsources.com/si/AS/Suzhou-Unitek/6008841872222/pdtl/Microwave-Motion-Sensor/1060027580.htm>

⁶ http://www2.clipsal.com/cis/technical/product_groups/energy_management/ultrasonic_motion_detectors

Research conducted for this study indicates that microwave motion sensors are used as occupancy sensors for lighting applications, as opposed to security applications. Therefore, this chapter focuses primarily on PIR and ultrasonic motion sensors.

4.3.1.2 How the Technology is Used

Schools use motion sensors of all types to detect and provide an alert when an individual enters a hall, classroom, or other unauthorized location. These are usually associated with rules such as the time of day (e.g., after school hours) when people should not be occupying or entering a given location. These types of sensors, irrespective of the specific scientific principle upon which they are based, detect the motion of an intruder in a vacant location where there should be no occupant during a specified time. Figure 4-2 shows the basic logic embedded in the sensor.



15-03015-019

Figure 4-2 Motion Detection Process

The first task is for a school staff member to activate the motion sensor (step 1). This task can also be done automatically by using the control panel to establish daily on/off hours of the motion sensor. The motion sensor will then establish baseline readings for the empty room (step 2) and continuously take these readings to ensure they are not changing. Once the readings are constant, the motion sensor will monitor the room (step 3). If an intruder enters the room (step 4), the sensor will detect the motion (step 5) and trigger the alarm (step 6).

Often motion sensors are mounted in the top corner against a wall, as shown in Figure 4-3.^{7,8}

Mounting motion sensors in this top corner optimizes two things. First, the sensor has the largest detection area for the best line of sight. Secondly, this sensor location is not obviously noticeable by the room occupants.⁹

⁷ <http://www.ackermansecurity.com/resources/blog/best-practices-for-placing-motion-detectors>

⁸ <http://www.home-security-systems-answers.com/motion-detector-wiring.html>

⁹ <http://www.safewise.com/blog/effective-placement-can-prevent-a-burglary-where-your-sensors-should-go/>

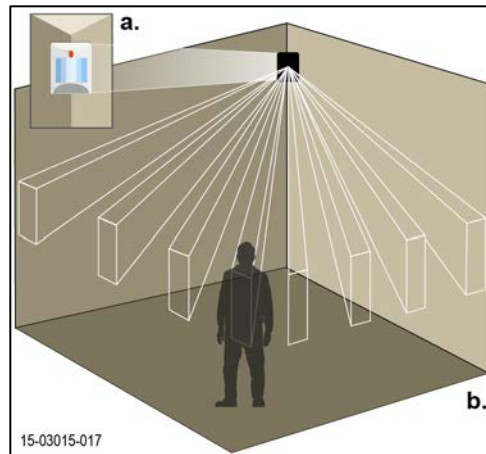


Figure 4-3 Corner-Mounted Motion Sensor Location¹⁰ and Detection Area¹¹

Another common location to mount motion sensors is on the ceiling.¹² This creates a cone-shaped detection area, which may leave room corners unprotected, as shown in Figure 4-4.

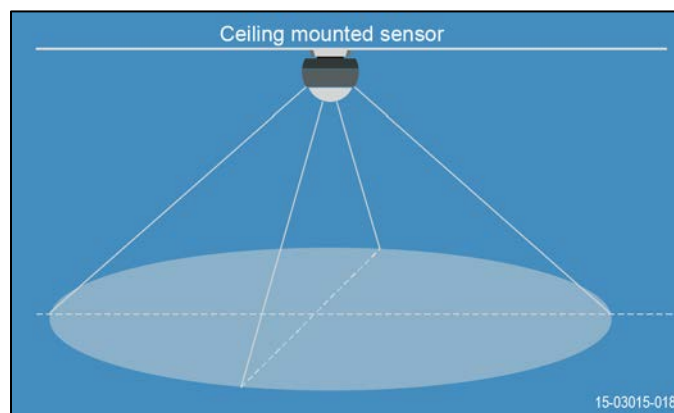


Figure 4-4 Detection Area for Ceiling-Mounted Motion Sensors¹³

If an intruder breaks into an alarmed location, he/she frequently looks for a motion detector and alarm system. Because many sensors are placed along the wall, intruders often look for them there. Installing sensors in the ceiling may be a less obvious location.¹⁴

¹⁰ <https://pixiescorner.wordpress.com/tag/2420m/>

¹¹ <http://www.diycontrols.com/p-6225-rokonet-wisdom-wireless-pet-immune-pir-motion-sensor.aspx>

¹² <https://www.ncjrs.gov/pdffiles1/Digitization/206415NCJRS.pdf>

¹³ <http://aeotec.com/z-wave-sensor/47-multisensor-manual.html>

¹⁴ <http://www.safewise.com/blog/effective-placement-can-prevent-a-burglary-where-your-sensors-should-go/>>

4.3.1.3 What Makes the Technology Good?

4.3.1.3.1 How the Technology Works

All of the motion sensors discussed have the same general principle: detect the motion of people. However, there are slight differences in how each of the motion sensor technologies work.

- **PIR sensors:** These motion sensors operate by passively reading the thermal energy emitted in a room. The sensor detects the temperature of a person and compares this against the background temperature in the room. When the temperature change is greater than an established threshold, the sensor triggers an alarm.
- **Active ultrasonic motion sensors:** Ultrasonic motion sensors actively emit pulses of acoustic sound energy. The energy pulses reflect off surfaces of the room and return to the motion sensor. When a person enters the room, the energy pulses are altered (commonly referred to as the “Doppler effect”), indicating there is movement in the room.

4.3.1.3.2 Differentiators

Passive motion sensors (such as the PIR) are a popular technology because of the cost associated with their use. Because a passive motion sensor does not actively emit energy pulses, it naturally uses less energy. However, their disadvantage is that they require a direct line-of-sight to the intruder. Active motion sensors (such as the ultrasonic) require more energy to actively emit pulses and are more expensive to use. However, because they actively emit energy pulses, they do not require a direct line-of-sight to the intruder.

Motion sensor performance varies from manufacturer to manufacturer. The primary considerations in choosing motion sensors include the following:

- **Detection area:** The detection area is the amount of square footage area covered by the motion sensor. A larger detection area requires fewer the motion sensors to cover the area.
- **Minor and major motion detection:** Minor motion detection is the ability to sense small movements, such as hand gestures, and is applicable for smaller rooms where people are generally sitting/standing. Major motion detection is the ability to sense larger movements, such as walking, and is applicable for larger rooms and transit areas where people are likely to be walking/moving.
- **False alarms:** Motion sensors, while very effective, can be susceptible to false alarms. The best motion sensors have specific features to minimize false alarms, such as ignoring small animals weighing less than specified weight. Other motion sensors take the approach of using multiple technologies (also known as dual-tech). This helps minimize the susceptibility of a single detection technology.
- **Field of view:** The FOV equates to how wide of an angle the motion sensor can detect. The wider the FOV, the more area and coverage the motion sensor has.

4.3.1.3.3 Specifications and Features

Table 4-3 provides a range of specifications for motion sensors. The specifications give specific metrics for comparing different types of motion sensors.

Table 4-3 Technical Specification Considerations for Motion Sensors

Dimensions (PIR)	
Length	1.7 to 2.5 in (42 to 64 mm) ^{15, 16}
Width	2.5 to 2.75 in (64 to 70 mm) ^{15, 16}
Height	3.5 to 5.0 in (89 to 127 mm) ^{17, 18}
Dimensions (Ultrasonic)	
Diameter	4.5 to 4.8 in (114 to 122 mm) ^{19, 20}
Height	1.4 to 1.5 in (35 to 38 mm) ^{19, 20}
Power Supply (PIR)	
Wired	9 to 15 volts direct current (VDC) at 10 to 18 mA ¹⁸
Wireless	9 VDC (battery life 6 months to 5 years) ^{16, 21}
Power Supply (Ultrasonic)	
Wired	10 to 30 VDC at 25 to 40 mA ^{22, 23}
Wireless	None
Connections	
Wired	Alarm panel
Wireless (radio)	Alarm panel
Wireless [Internet Protocol (IP)]	Alarm panel, other Internet-based devices
Specifications (PIR)	
Operating temperature	–30 to 140 °F (–34 to 60 °C) ^{16, 17}
Relative humidity, non-condensing	0 to 95% ¹⁸
Detection area coverage	40×56 ft (12×17 m) to 50×70 ft (16×21 m) ^{15, 18}
Detection range	12 to 50 ft (3 to 15 m) ^{16, 24}
Detection angle	20 to 100 degrees ¹⁶
Specifications (Ultrasonic)	
Operating temperature	32 to 104 °F (0 to 40 °C) ¹⁹
Detection angle	0 to 360 degrees ²⁰
Detection frequency	32 kHz or 40 kHz ²²
Minor detection area coverage	14×18 ft (4×5 m) to 46×24 ft (14×7 m) ^{25, 22}
Major detection area coverage	20×26 ft (6×7 m) to 32×64 ft (9×19 m) ²⁵

¹⁵ https://www.elvessupply.com/Aleph-AL40-40X40-Detection-100Lb-Pet-Immune_p_1238234.html?gclid=CPbwoLDmnMgCFdgHgQodOoEHNA#tab-8

¹⁶ <https://www.dakotaalert.com/docs/IR-2500%20Manual%20-%20web.pdf>

¹⁷ <http://www.dsc.com/alarm-security-products/BV-300%20-%20Digital%20Bravo%20AE%20300%20PIR%20Motion%20Detectors%20BV-300/1332>

¹⁸ http://resource.boschsecurity.com/documents/ISC_PPR1_W16_Data_sheet_enUS_9007201854188299.pdf

¹⁹ <http://www.lutron.com/TechnicalDocumentLibrary/LOS-CUS%20Series.pdf>

²⁰ <http://www.wattstopper.com/products/sensors/ceiling-or-wall-mount-sensors/wt.aspx#.Vfr1KaPD9D8>

²¹ <http://www.interlogix.com/intrusion/product/ds924i-motion-sensor/>

²² http://www.cooperindustries.com/content/dam/public/lighting/controls/products/documents/greengate/spec_sheets/oac_u_line_spec_sheet.pdf

²³ <http://www.wattstopper.com/products/sensors/ceiling-or-wall-mount-sensors/wt.aspx#.Vfr1KaPD9D8>

²⁴ http://www.interlogix.com/_assets/library/108-3451_wall_mount_sensors_ds.pdf

²⁵ http://www.bryant-electric.com/literature/BLBHM001_H-MOSS.pdf

Table 4-3 Technical Specification Considerations for Motion Sensors (Continued)

Features (PIR)
Low-battery alert (wireless models only) ¹⁶
Multi-level PIR signal processing ¹⁷
Pet immunity up to 85 pounds ²⁶
Features (Ultrasonic)
Angled transmitter and receiver pairs help optimize sensitivity while eliminating unwanted detection from ceiling air movement ²⁰
Dual in-line package switch-adjustable time delay and sensitivity ²⁰
Light-emitting diode (LED) indicates occupancy detection ²⁰
Temperature and humidity resistant receivers ²⁰

4.3.1.3.4 Effectiveness

One of the most frequent uses for motion sensors is to save energy by keeping lights off when the room is unoccupied and use motion sensors to turn lights on when someone enters the room. For security applications, this same function is also one of the best ways to enable early detection of intruders, but the placement is critical to success. To successfully use these sensors, they should be placed at the most effective routes of ingress and egress.⁹

4.3.1.3.5 Policy Impacts

Schools will need to document the placement and usage of motion sensors in an emergency response plan. It is important to understand how alarms should be processed, for example once an alarm is received at an alarm box, should local law enforcement be automatically notified, or should school personnel be notified and make the decision to call law enforcement? Moreover, it is important to have pre-identified policies for the actions to be taken by all interested stakeholders upon receipt of an alarm notification.

4.3.1.4 Concerns About the Technology

4.3.1.4.1 What It Does Not Do

PIR motion sensors have some limitations in their detection abilities. Firstly, they require a direct line-of-sight. If an intruder is outside the detection area of the PIR motion sensor, no alarm will be triggered. Additionally, PIR motion sensors depend on a difference in temperature readings. As the temperature of the environment approaches the temperature of a moving intruder (e.g., 98 °F), it will become increasingly difficult for the sensor to detect the difference in thermal energy readings.

Ultrasonic motion sensors also have limitations. They rely on sound waves reflecting off hard objects. Because acoustic waves do not reflect off soft objects well, the sensor might not detect some soft objects, such as foams or fabrics.²⁷

Another limitation is the speed of the motion. The intent of a motion sensor is to sense motion of an intruder in a room. The threshold that triggers the alarm is the speed of the motion. If the intruder

²⁶ <http://www.dsc.com/index.php?n=products&o=view&id=106>

²⁷ <http://www.securitymagazine.com/articles/79070-mythbusters-are-busted-1>

moves more slowly than the sensor's threshold, the sensor may not recognize the intruder as a viable moving object.

Motion sensors are generally unable to distinguish how many moving objects are occupying a room. The feedback received from a motion sensor indicates whether or not there is motion. There is no delineation between multiple moving objects. Motion sensors also have a limited FOV. Therefore, it is important to carefully consider where and how to mount motion sensors.

4.3.1.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

While effective, most motion detectors use infrared to detect significant changes in the surrounding room's temperature and thus can be vulnerable to efforts to intentionally minimize or hide temperature changes.²⁸ Some types of ultrasonic motion sensors can be reset or temporarily blinded by pointing a source of infrared or near infrared light at them.²⁹

PIR motion sensors essentially measure the temperature of a moving person, as compared to the background temperature of the environment. The closer the temperature of the background environment to the temperature of the human body temperature, the harder it is to delineate between the environment and the intruder. This limitation leads to the possibility that an intruder could enter a very warm room undetected.

4.3.1.4.3 Possibilities for Misuse

Other than the possibility of intentionally triggering motion detectors as a prank or to cause a nuisance, no instances of misuse were identified.

4.3.1.4.4 Liability and Safety Concerns

No immediate liability or safety concerns were identified.

4.3.1.4.5 Privacy Concerns

Motion sensors do not actively record a log; therefore, there are no privacy concerns. In fact, motion sensors can often be used in locations where privacy is an issue.

4.3.1.4.6 Accommodations Needed for Disabilities

The author did not identify any disability accommodation issues.

4.3.1.4.7 Other Issues

As previously discussed, some motion sensors are designed with a pet-immunity feature so that movement from an object smaller than a certain size does not trigger an alarm. This feature should be used carefully because children in elementary schools may be of too small to trigger these types of alarms.

²⁸ <http://www.csoonline.com/article/2133815/physical-security/researchers-show-ways-to-bypass-home-and-office-security-systems.html>

²⁹ http://www.residential-landscape-lighting-design.com/2005_11_01_outdoor_lighting_archive.html

4.3.1.4.8 Policy Concerns

No policy concerns were identified by the author.

4.3.1.5 Cost Considerations

Table 4-4 presents the various costs that may be associated with motion sensors.

Table 4-4 Motion Sensor Cost Considerations

Cost Factor	Cost Description
Acquisition (PIR)	PIR motion sensors can cost \$8.75 to \$14.38 per unit to \$64.99 to \$69.99 per unit.
Acquisition (ultrasonic)	Ultrasonic motion sensors can cost \$53.95 to \$162.00 for basic units and \$119.99 to \$170.92 for more advanced units.
Exceptional installation costs	Wired motion sensors require special 22-gauge, four-conductor wiring installation.
Operation and labor	None; motion sensors are intended to be automated.
User training	School officials will need to provide training for school staff on the presence and locations of motion sensors.
Maintenance	Little to none. Motion sensors are manufactured to be installed and require minimal ongoing maintenance (unless they require a battery). School staff should periodically test motion sensors to ensure they are working properly.
Consumables	Wireless battery-powered motion sensors will require periodic battery replacement, according to the battery usage requirements. Some motion sensors incorporate a low-battery strength indicator.
Energy and energy dependency	Wired motion sensors should be connected to the central alarm panel and receive power from the facility power grid. PIR motion sensors should consume less power than active motion sensors because they do not actively emit energy pulses. When integrated into facilities correctly, motion sensors can reduce the facility's energy usage by deactivating lighting in unoccupied rooms.
Software licenses	Motion sensors connect to the alarm panel, which can control all the sensors components; it should come with software pre-installed. Motion sensors should not require software installation.
System integration	Motion sensors connect directly to the alarm panel. Connections can be either wired or wireless, depending on the motion sensor and the alarm panel. Motion sensors may or may not connect to cameras for added surveillance.

4.3.1.6 Emerging Technologies and Future Considerations

There are smart cameras that can also act as motion sensing devices. These smart cameras use image processing to detect what is happening in an image and analyze what people are doing. See Chapter 9 for additional information on smart cameras.

Sensors also exist to detect chemical, biological, and radiological/nuclear (CBRN) hazards. While these hazards are very real for schools in active war zones around the world, U.S. schools have not yet confronted these types of threats. The author did not find any evidence of the use of CBRN sensors by schools in the United States; therefore, such sensors are not discussed in this report.

4.3.1.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 4-5 provides examples of known vendors of motion sensors; however, it is not comprehensive and other vendors may exist. The list is current as of 20 December 2015.

Table 4-5 Motion Sensor Vendors

Vendor	Website
Bosch Security Systems	https://us.boschsecurity.com
Dakota Alert, Inc.	https://www.dakotaalert.com
Digital Security Controls	www.dsc.com
Aleph America	www.aleph-usa.com
GE Interlogix (a UTC Fire and Security Company)	www.interlogix.com
WattStopper	www.wattstopper.com
Lutron	www.lutron.com
Hubbell Bryant	www.bryant-electric.com
Cooper Lighting	http://www.cooperindustries.com/content/public/en/lighting.html
Leviton	www.leviton.com
Pepperl+Fuchs	http://www.pepperl-fuchs.us

4.3.2 PHOTOELECTRIC BEAM SENSORS

4.3.2.1 Introduction




Like motion sensors, photoelectric beam sensors are employed in schools to detect the presence of an intruder crossing a specified perimeter. Photoelectric beam sensors use optical technology to detect people or objects crossing into an established perimeter. The type of light beam varies from one vendor's sensor to another. Some photoelectric beam sensors use laser light, whereas others use infrared light emitted by LEDs. The photoelectric beam sensors discussed in this chapter, including through-beam sensors, retro-reflective sensors, and diffuse-reflective sensors, are displayed in Table 4-6. Figure 4-5 illustrates the principles of each sensor type.

4.3.2.2 How the Technology Is Used

The operational objective of photoelectric beam sensors is to monitor a perimeter or opening and detect the presence of an object crossing a line defined by a light beam. Figure 4-6 shows the process for perimeter monitoring.

Once the sensor enters a state where motion into or across the line monitored by the photoelectric beam should generate an alarm, the sensor monitors the space (step 1) and establishes a normal or baseline state. If an intruder crosses the invisible perimeter (step 2) and the beam is broken for an interval that exceeds a predefined setting, the sensor will detect the broken beam (step 3) and trigger the alarm (step 4).

Table 4-6 Examples of Photoelectric Beam Sensors

Photoelectric Beam Sensor Type	Description	Example
Through-beam	Uses two units. The active unit emits a beam of light and the receiving unit detects the incoming light. Under normal conditions, the units will emit and detect the beam. However, when an object moves between the units and blocks the light beam, the receiving unit will no longer detect the light beam, thus indicating the presence of the person or object. This action will create an alarm.	 30
Retro-reflective	Uses one active unit and one reflecting unit. The light is emitted from one unit and reflected back to the original emitting unit, which then detects the light. Again, when a person or object obstructs the path of the light beam, the unit will no longer detect the light and will generate an alarm.	 31
Diffuse-reflective	Uses a single unit. This unit combines the beam emitting and beam detecting capabilities into a single unit. Under normal conditions, the unit emits the beam into open air. However, when an object moves into the path of the beam, the beam reflects off the object's surface back toward the receiving unit, allowing the beam to make a complete path from the sender to the receiver. This differs from the previous two sensors in that the detection of the presence of the return beam is what triggers the alarm, as opposed to the absence of the beam.	 32

³⁰ <http://uk.rs-online.com/web/p/photoelectric-sensors/1149982/>

³¹ <http://salestores.com/secolarme93108.html#.VehWwaPD9D8>

³² [http://www.automationdirect.com/ad/Shopping/Catalog/Sensors_-z-_Encoders/Photoelectric_Sensors/DC_Rectangular/Retroreflective_for_Transparent_Objects_\(QM_Series\)/QMIG-0P-0A?utm_source=google&utm_medium=product-search&gclid=COuLrfC5oswCFYJZhgodaN4BFA](http://www.automationdirect.com/ad/Shopping/Catalog/Sensors_-z-_Encoders/Photoelectric_Sensors/DC_Rectangular/Retroreflective_for_Transparent_Objects_(QM_Series)/QMIG-0P-0A?utm_source=google&utm_medium=product-search&gclid=COuLrfC5oswCFYJZhgodaN4BFA)

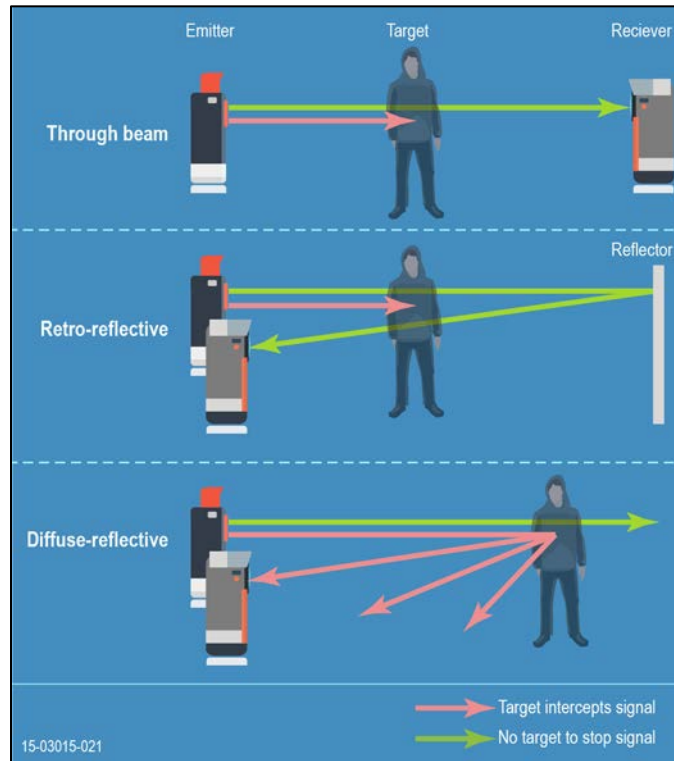


Figure 4-5 Photoelectric Beam Detector Types

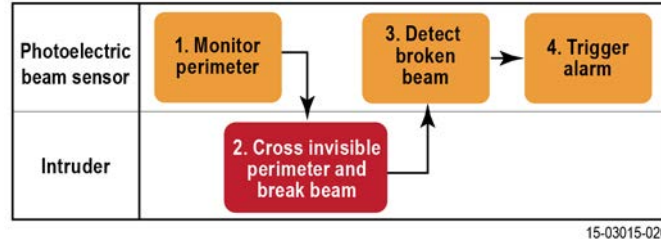


Figure 4-6 Photoelectric Beam Process

4.3.2.3 What Makes the Technology Good

4.3.2.3.1 How the Technology Works

Irrespective of the configuration of photoelectric beam sensors, one unit or two units, when an individual crosses a beam of light, an alarm is generated. Photoelectric beam sensors are used for outdoor and indoor applications, as shown in Figure 4-7. Outdoor photoelectric beam sensors are typically installed either near building entrances or away from buildings near fence perimeters.³³ Indoor photoelectric beam sensors are installed near doorways or hallway entrances.³⁴ By using these installation locations, a school can monitor its outdoor perimeter around the facility, whereas the indoor setup can monitor the entrance to a specific room.

³³ <http://www.enforcer.com.tw/burglar/CRTSN.htm>

³⁴ Ibid

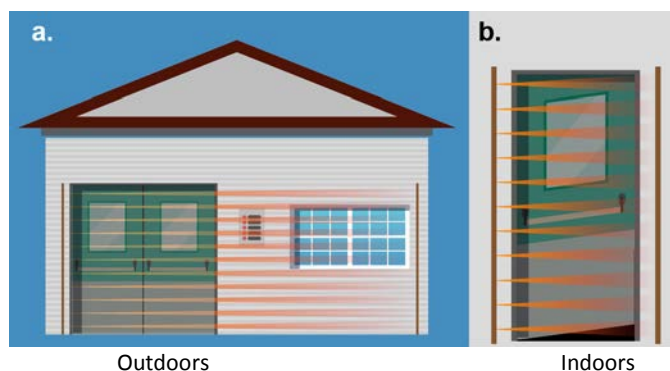


Figure 4-7 Photoelectric Beam Installation Used Outdoors and Indoors

4.3.2.3.2 Differentiators

The performance of photoelectric beam sensors varies from one manufacturer to another. The key factors to compare include:

- **Detection range:** The detection range is the distance from the light-sending unit and the potential target. Units often have a different standard for indoor and outdoor detection ranges. Greater detection ranges can build larger perimeters, but may be more susceptible to false alarms.
- **Reduction of false alarms:** Photoelectric beam sensors are susceptible to objects moving between the beams and setting off a false alarm. These objects can include trash, leaves and branches, or animals, and are primarily a concern for outdoor applications. Some photoelectric beam sensors feature multiple beams (common models are either dual-beam or quad-beam). Multiple-beam sensors are designed to trip an alarm only when all beams are broken, making false alarms less likely.
- **Alignment angle:** The alignment angle refers to the degree to which the sensors can be adjusted horizontally and vertically, once mounted. The greater the alignment angle, the more flexible the mounting options for the sensors. Note: the alignment angle is non-applicable to Diffuse-Reflective sensors.
- **Response time:** The response time is the amount of time the beam can be broken (usually in milliseconds) before the sensor will trigger an alarm. This feature is generally adjustable for photoelectric beam sensors. Shorter response times are more sensitive to detecting intruders, but are also more susceptible to triggering false alarms.

4.3.2.3.3 Specifications and Features

Table 4-7 provides a range of specifications for photoelectric beam sensors. The specifications give specific metrics for comparing different types of photoelectric beam sensors.

Table 4-7 Technical Specifications for Photoelectric Beam Sensors

Dimensions	
Depth	1.1 to 4.3 in. (29 to 110 mm) ^{38, 35}
Width	2.3 to 4.4 in. (59 to 113 mm) ^{37, 35}
Height	3.3 to 15.6 in. (86 to 398 mm) ^{37, 40}
Power Supply	
Wired	10 to 30 volts alternating current (VAC) or VDC ³⁶
Wireless	3.6 VDC (typical lifespan 3 to 5 years) ³⁷
Connections	
Wired	Alarm panel
Wireless (radio)	Alarm panel, other photoelectric sensors
Wireless (IP)	None
Specifications	
Operating temperature	–31 to 151 °F (–35 to 66 °C) ³⁹
Detection range	100 to 2000 ft (30 to 500 m) ^{38, 39}
Response time	35 to 700 ms ⁴⁰
Horizontal alignment angle	5 to 180 degrees ^{38, 41}
Vertical alignment angle	5 to 24 degrees ^{36, 42}
Features	
For indoor and outdoor use. ³⁸ Multiple beams provide perimeter security, minimizing false positives from environmental causes (e.g., falling leaves, birds). ³⁶ Lensed optics reinforce beam strength and provide immunity to false alarms caused by rain, snow, mist, etc. ³⁶ Multi-frequency; selectable beam frequencies can eliminate interference between multiple units. ⁴³ Audible beam alignment (buzzer), beam strength indicator, and laser alignment make transmitter and receiver alignment faster. ⁴³	

4.3.2.3.4 Effectiveness

There are several ways to help optimize the performance of these devices. Using multiple-beam sensors will mitigate false-positive readings. Manufacturers make photoelectric beam sensors that emit single, dual, or quad beams of light. The dual- and quad-beam sensors require all beams of light to be broken for the sensors to trigger the alarm.⁴⁴

³⁵ <http://www.seco-larm.com/pdfs/PI-QuadPhotoBeam.pdf>

³⁶ <http://www.seco-larm.com/E960LRb.htm>

³⁷ <http://www.optexamerica.com/security-products/ax-200tfri>

³⁸ <http://www.seco-larm.com/E961S90W.htm>

³⁹ <http://www.optexamerica.com/security-products/ax-200tn>

⁴⁰ https://us.boschsecurity.com/us_product/products/intrusionalarmsystems/detectorsandaccessories/photoelectricbeam/ds484qandds486qquadbeamph/ds484qandds486qquadbeamph_5142

⁴¹ <http://www.security.honeywell.com/hsc/products/intruder-detection-systems/sensor/photoelectric-beam/19035.html>

⁴² <http://library.ademconet.com/MWT/fs2/0-000-141-01/Intellibeam-Dealer-Data-Sheet.PDF>

⁴³ <http://www.seco-larm.com/pdfs/PI-QuadPhotoBeam.pdf>

⁴⁴ <http://www.enforcer.com.tw/burglar/CRTSN.htm>

Photoelectric beam sensors can also be used in combination with cameras. Photoelectric beam sensors can trigger notifications to officials to pay attention to a specific location or, if appropriately integrated, cause surveillance cameras to rotate and focus on the location of the triggering incident.

4.3.2.3.5 Policy Impacts

Schools will need to document the placement and usage of photoelectric beam sensors in an emergency response plan, including how security should respond to an alarm, and who should be notified.

4.3.2.4 Concerns About the Technology

4.3.2.4.1 What It Does Not Do

Because they are sometime used to protect a perimeter, photoelectric beam sensors are commonly referred to as “invisible fences.” Such invisible fences merely detect when a threat has entered the perimeter but do not create a physical barrier like a fence. Intruders are still able to enter onto a school property that does not have a physical fence.

There is limited feedback from the device. When a person or object breaks the beam, the sensor is incapable of sensing the type, size, number, or color of the object(s) blocking the beam.

Another shortfall of photoelectric beam sensors is their FOV. Because the beam travels in a straight line, a single photoelectric beam sensor is incapable of monitoring, for example, an entire room.

Lastly, environmental conditions can pose significant challenges to photoelectric sensors. Wind, rain, snow, and fog can create false alarms rendering these devices less useful in some locations.

4.3.2.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Although popular movies may suggest that a flashlight or television remote can be used to replace and thus circumvent a photoelectric beam “this type of tampering will not work on properly designed and engineered higher-end products.”⁴⁵ If an intruder knows where the sensors are located, it may be possible to jump over or otherwise avoid breaking the beam.

4.3.2.4.3 Possibilities for Misuse

None identified by the author.

4.3.2.4.4 Liability and Safety Concerns

Because photoelectric beam sensors cannot prevent someone from entering or exiting the perimeter, they should not be used in situations where it is critical to keep people on one side of a boundary, such as preventing children from exiting school property and entering a dangerous roadway.

4.3.2.4.5 Privacy Concerns

Photoelectric beam sensors do not record activity; therefore, there are no inherent privacy concerns however, these sensors may be used to trigger a recording device, in which case it is important to consider who will have access to such recordings and how they will be analyzed and stored.

⁴⁵ <http://www.securitysolutionsmagazine.biz/2013/12/04/understanding-electronic-perimeter-protection/>

4.3.2.4.6 Accommodations Needed for Disabilities

The author did not identify any disability accommodation issues.

4.3.2.4.7 Policy Concerns

No policy concerns were identified by the author.

4.3.2.5 Cost Considerations

Table 4-8 discusses the various costs that may be associated with photoelectric beam sensors.

Table 4-8 Photoelectric Beam Sensor Cost Considerations

Cost Factor	Cost Description
Acquisition (Single Beam)	Single photoelectric beam sensors cost \$49.00 to \$74.95 for basic units and \$140.00 to \$215.00 for more advanced units.
Acquisition (Dual Beam)	Dual photoelectric beam sensors cost \$69.00 to \$97.95 for basic units and \$222.44 to \$331.95 for more advanced units.
Acquisition (Quad Beam)	Quad photoelectric beam sensors cost \$227.44 to \$496.95 for basic units and \$289.45 to \$647.99 for more advanced units.
Exceptional installation costs	Wired models will require that wiring be run to the units. For outdoor units, this may entail burying underground wire to the units.
Operations and labor	Monitoring or response to an alarm.
User training	Little to none. School staff should be made aware of the photoelectric beam sensors, but should not require any kind of special training.
Maintenance	Sensors mounted outside may be subject to environmental elements, such as dust, dirt, snow, and fog. Therefore, the sensors may require periodic cleaning and maintenance to ensure they are operating at peak performance. Schools should service sensors regularly to minimize the chances of false alarms.
Consumables	Some photoelectric beam sensors are wireless and therefore will require batteries that will need to be periodically replaced. Correctly designed sensors should include a low-battery indicator.
Energy and energy dependency	Wired models will connect directly to and receive power from the alarm panel. Wireless models will be battery powered and will required periodic battery replacement.
Software licenses	None
System integration	Photoelectric beam sensors connect directly to the alarm panel. Connections can be wired or wireless.

4.3.2.6 Emerging Technologies and Future Considerations

Current photoelectric sensors use infrared light, but manufacturers are exploring other forms of technology to establish invisible perimeter protection, such as microwave technology. The intent of using microwaves is to mitigate the effects of environmental conditions that can cause false alarms.⁴⁶

⁴⁶ <http://www.sdmmag.com/articles/83459-microwave-perimeter-protection-affordable>

4.3.2.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 4-9 provides examples of known vendors of photoelectric beam sensors; however, it is not comprehensive and other vendors may exist. The list is current as of 4 November 2015.

Table 4-9 Photoelectric Beam Sensor Vendors

Vendor	Website
SECO-LARM USA, Inc.	http://www.seco-larm.com/
Bosch Security Systems	https://us.boschsecurity.com/
ADEMCO (a Honeywell Company)	http://www.ademco.eu/
Optex	http://www.optex.co.jp/e/
Pepperl+Fuchs	http://www.pepperl-fuchs.us
TAKEX	http://takex.com/

4.3.3 OPEN-DOOR SENSORS

4.3.3.1 Introduction

A locked door might not stop a determined intruder, but doors routinely left open can expose building occupants to unacceptable security breach risk. Open-door sensors are devices that attach to a door and indicate whether the door is open or closed. Open-door sensors discussed in this report include magnetic sensors and contact sensors, as shown in Figure 4-8.

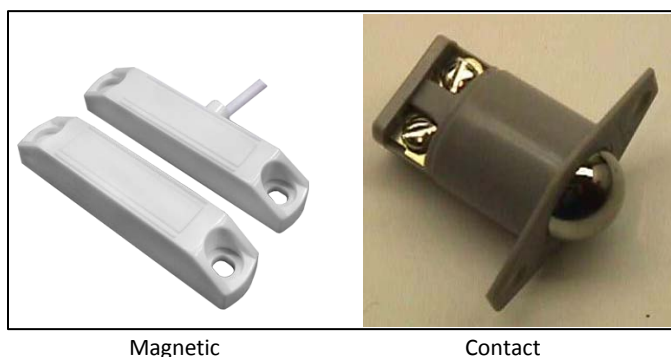


Figure 4-8 Door Open Sensors for Magnetic⁴⁷ and Contact⁴⁸

Schools use door sensors on doors that may be used for routine entry or exit, e.g., those leading to the playground but that should not be held or propped open during school hours. These devices often rely on a magnetic switch, with one piece attached to the doorframe and another piece attached the door itself. When the two parts are separated for more than a preset amount of time, the sensor triggers an alarm.

These devices could also be installed on windows and operate identically.

⁴⁷ http://www.kasonind.com/index.php/products/lighting_and_electrical/electrical_supplies/1967-8-door-open-sensor/

⁴⁸ http://www.residential-landscape-lighting-design.com/2005_11_01_outdoor_lighting_archive.html

4.3.3.2 How the Technology Is Used

A common access control concern for schools is having staff, teachers, or students prop open an exterior door while performing a brief task outside such as making a private phone call or investigating something outside. A door may also fail to latch completely, leaving the school open to intruders. Whether accidental or intentional, open doors circumvent other security measures and provide a means of potential entry to the school. Open-door sensors help enforce existing access control systems and policies by generating an alert when a door opens that is not supposed to or remains open longer than necessary for routine use.

The operational objective of open-door sensors is to ensure the external doors are closed, thereby preventing unauthorized intruders from entering school property. Figure 4-9 show a general process for open-door sensors.

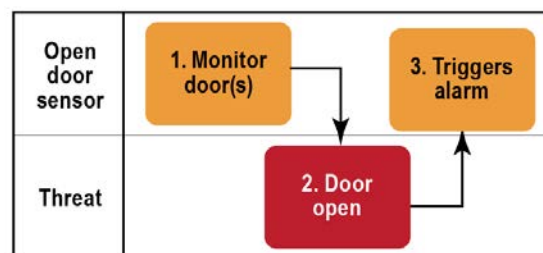


Figure 4-9 Open-Door Process

First, the sensor monitors the door (step 1) and establishes a baseline condition. Once a monitored door is opened (step 2), the sensor triggers an alarm (step 3). Different scenarios can trigger an alarm in this manner: an unauthorized individual opens the door or a school occupant opens the door and leaves it open. If an alarm is triggered in this manner and the system is monitored, school staff can investigate the cause of the alarm.

Open-door sensors have two components mounted on the door and its frame. The first is the sensor itself, which is mounted to the doorframe, as shown in Figure 4-10. The second component is the magnet that is detected by the sensor, also shown in Figure 4-10. Open-door sensors can also be mounted inside of the door and doorframe, thereby hiding the sensor. Once mounted, the open-door sensor works automatically, requiring no human involvement for intruder detection.



Figure 4-10 Open-Door Sensors Mounted to Door⁴⁹

4.3.3.3 What Makes the Technology Good

4.3.3.3.1 How the Technology Works

Door sensors may use a magnetic switch to create a closed electric circuit. If someone opens an armed door or window, the magnet is pulled away from the switch, which breaks the circuit and triggers an event such as sending an electronic message or initiating an alarm sound.⁵⁰ With a contact sensor the closed door depresses a mechanical plunger. When the door is opened, the plunger is released, indicating the door has been opened.

Doors used during normal business hours but intended to be opened and closed promptly should have sensors that use a timer. Used in this way, the sensor generates an alert only after a door has been left open for an extended period of time. Consideration should be given to determining how many people routinely pass through the door in succession and a realistic duration for them to do so. Circumstances may be different during the day, e.g., when a bus drops off students, the front door is likely to remain open as students file through; however, later in the day it is more likely only one or two visitors will pass through the door together. It may be necessary to have an override for doors that are occasionally opened for an unusual length of time, such as those leading to a loading dock or trash area. An additional tamper alert should be considered if there is potential for people to attempt to disable the sensor.

Sensors can trigger a local alarm, generate an alarm at a remote alarm panel, or send a notification via Wireless Fidelity (WiFi), cellular, or other telecommunications network. If the alarm is merely intended to enforce an access policy by generating a loud noise when someone uses a door that is expected to stay closed, an inexpensive wireless door alarm may suffice. Such a device cannot send a notification and it may be easily disabled, but it is an effective reminder. If there is concern about unauthorized access from outside, a more robust alarm with the ability to send a notification should be considered.

⁴⁹ <https://robots.thoughtbot.com/arduino-bathroom-occupancy-detector>

⁵⁰ <http://simplisafe.com/blog/door-sensor-secrets>

4.3.3.3.2 Differentiators

Open-door sensors are simple devices. However, there are two contributing factors one should consider when comparing performance between products:

- **Gap distance:** The gap distance is the distance the magnet (attached to the door) and the sensor (attached to the doorframe) can move away from each other before the sensor detects the door has been opened. In similar fashion, the gap distance is the distance the door must travel before the plunger is released in a contact sensor arrangement. A smaller gap distance makes it more difficult for intruders to circumvent the sensor.
- **Concealment:** Some open-door sensors are hidden inside the door or doorframe. Concealing the sensor has two advantages. First, the individual may not be aware of the presence of open-door sensors, allowing officials to respond without the intruder knowing. Second, a concealed open-door sensor is more difficult to reach, making it harder for an intruder to circumvent the technology, if he/she is aware of its presence.

4.3.3.3.3 Specifications and Features

Table 4-10 presents a range of specifications for open-door sensors. The specifications provide specific metrics for comparing different types of open-door sensors.

Table 4-10 Technical Specifications for Open-Door Sensors

Dimensions (Magnetic)	
Length	1.07 to 4.33 inches (27 to 111 mm) ^{51, 52}
Width	0.33 to 1.75 inches (8 to 44 mm) ^{51, 52}
Height	0.16 to 0.50 inches (4 to 13 mm) ⁵¹
Dimensions (Contact)	
Diameter	0.75 to 0.85 inches (15.9 to 19.3 mm) ^{53, 54}
Length	0.33 to 3.4 inches (8 to 87 mm) ^{53, 55}
Power Supply (Magnetic)	
Wired	Powered by alarm panel
Wireless	3 VDC (battery life 3 to 5 years) ^{56, 57}
Power Supply (Contact)	
Wired	Powered by alarm panel
Wireless	3 VDC (battery life: 6 months to 7 years) ^{55, 53}

⁵¹ <http://www.nascominc.com/n135wgw-st180-capc.html>

⁵² <http://www.seco-larm.com/Magnet4.htm>

⁵³ <http://www.security.honeywell.com/hsc/products/intruder-detection-systems/wireless/door-window-sensor/306943.html>

⁵⁴ <http://www.vellemanusa.com/products/view/?country=us&lang=enu&id=351030>

⁵⁵ <http://www.smarthome.com/insteon-2845-222-hidden-door-sensor.html>

⁵⁶ <http://www.oemsensors.com/products/wifi-sensors/open-closed.php>

⁵⁷ <http://us.sourcesecurity.com/technical-details/access-control/accessories.2/accessories/assa-abloy-aperio-aperio-sensor-as100-access-control-system-accessory.html>

Table 4-10 Technical Specifications for Open-Door Sensors (Continued)

Connections	
Wired	Alarm panel
Wireless (radio)	Alarm panel
Wireless (IP)	Alarm panel
Specifications (Magnetic)	
Operating temperature	–40 to 160 °F (–40 to 70 °C)
Gap distance	0.50 to 3.00 inches (13 to 76 mm)
Specifications (Contact)	
Operating temperature	–40 to 120 °F (–40 to 49 °C)
Gap distance	0.14 inches (3 mm)
Features	
Recesses into door and frame Rugged construction Surface mounting Transmits supervisory, tamper, and low battery alerts Case tamper protection	

4.3.3.3.4 Effectiveness

When deciding between types of open-door sensors, features to consider are the ability to adjust the time delay before the alarm activates, options to set times when the sensor is inactive, and notification options.

4.3.3.3.5 Policy Impacts

Schools purchasing open-door sensors should include this technology in the school policies. The policies and procedures will help ensure appropriate usage of the sensors. At a minimum, schools should document where the open-door sensors are installed and how school staff should respond to an alarm. Policies may also address corrective actions for doors being left open.

4.3.3.4 Concerns About the Technology

4.3.3.4.1 What It Does Not Do

Open-door sensors can help prevent unauthorized access, but they do not offer additional security during an incident. Open-door sensors can indicate when a door is opened or closed, but cannot indicate whether someone entered the door or window or passed something through it. Also, these sensors merely indicate when the door is opened or closed; they do not indicate whether the door is locked.

4.3.3.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

Intruders may attempt to override the open-door sensor. Magnetic open-door sensors may be thwarted using a separate magnet to keep the circuit closed while opening the door.⁵⁸ However, some sensors are resistant to this by having a two-way threshold. If the magnetic field is higher or lower than this threshold, the sensor will trigger the alarm. One could also detach the sensor from the doorframe and allow it to stay connected to the main sensor body.

A contact alarm could be circumvented by mechanically restricting the plunger from releasing.

Magnetic and contact sensors normally have a delay feature, and therefore it is possible for someone to quickly open the door, enter, and close the door without activating an alarm. These devices are often designed to deactivate if the door is closed after the alarm has been triggered, and thus do not provide a means to track unauthorized entry.

4.3.3.4.3 *Possibilities for Misuse*

If the alarm is activated frequently either as a prank or because policies are not enforced, there is the risk that the alarm will be disabled or ignored by someone inconvenienced by the disruption.

4.3.3.4.4 *Liability and Safety Concerns*

No immediate liability or safety concerns were identified.

4.3.3.4.5 *Privacy Concerns*

Because open-door sensors do not record the activity of individuals using the door, there are no privacy concerns.

4.3.3.4.6 *Accommodations Needed for Disabilities:*

Open-door sensors should integrate with existing automatic doors and should allow sufficient time for someone with mobility issues to pass through the door without triggering a false alarm.

4.3.3.4.7 *Policy Concerns*

The addition of open-door sensors is normally used to supplement existing policies that prohibit school occupants from leaving exterior doors propped open.

4.3.3.5 *Cost Considerations*

Table 4-11 presents the various costs that may be associated with open-door sensors.

⁵⁸ <http://www.csoononline.com/article/2133815/physical-security/researchers-show-ways-to-bypass-home-and-office-security-systems.html>

Table 4-11 Open-Door Sensor Cost Considerations

Cost Factor	Cost Description
Acquisition	\$30 to \$350 per unit, with installation hardware.
Installation	Varies with complexity of device selected. Basic models are simple electrical switches that are wired to the alarm panel. These basic models may, however, may require electrical wiring be installed inside the walls. More sophisticated models wirelessly broadcast the door position to the alarm panel. “Installation can be very complex for sensors which are integrated into an existing electrical system, alarm panel or access control system, requiring significant expenditures for installation.” ⁵⁹
Operation and labor	Because open-door sensors are designed to work autonomously, there should be little to no cost to have school staff operate the devices.
User training	Little to none. School staff should be made aware of the open-door sensors, but should not require any kind of special training.
Maintenance	School staff should periodically check and test the open-door sensors to ensure they operate appropriately.
Consumables	Wireless open-door sensors are battery powered. These battery-powered models will require periodic replacement of batteries. Some models send a low-battery indicator.
Energy and energy dependency	The alarm panel powers wired open-door sensors. Wireless open-door sensors are battery powered.
Software licenses	None.
System integration	Open-door sensors (both wired and wireless models) can connect directly to the control panel.

4.3.3.6 Emerging Technologies and Future Considerations

None identified by the author.

4.3.3.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 4-12 presents examples of known vendors of open-door sensors; however, it is not comprehensive and other vendors may exist. The list is current as of 15 October 2015.

⁵⁹ “Securitron Model DPA-12 and DPA-24 Door Prop Alarm Timers Installation and Operating Instructions.” Securitron Magnalock Corporation. Retrieved 28 September 2015 from http://www.securitron.com/Other/Securitron/_OWNA2.0/Documents/Installation_Instructions/Access_Control_Accessories/DPA-12_DPA-24_IO_500-15700%20C.pdf.

Table 4-12 Open-Door Sensor Vendors

Vendor	Website
Detex	http://www.detex.com/Products/LifeSafetySecurityDoorHardware/ExitAlarms/tabid/151/Default.aspx
Mace Wireless Door/Window Sensor	http://www.walmart.com/ip/Mace-Wireless-Door-Window-Sensor/10756574
Securitron/ASSA ABLOY	http://www.securitron.com/en/site/securitron/products/access-control-accessories/dpa-door-prop-alarm/
Nascom, Inc.	https://www.nascominc.com
GE Interlogix	http://www.interlogix.com/
SECO-LARM USA INC	http://www.seco-larm.com/
Honeywell	http://www.security.honeywell.com/
OEMSensors.com	http://www.oemsensors.com/
INSTEON	http://www.insteon.com/
Velleman	http://www.vellemanusa.com/

4.4 DURESS ALARMS






4.4.1 INTRODUCTION

A duress alarm in the context of school safety is a device used to send a warning signal when an intruder has been detected. Common duress alarms include panic buttons, badge alarms, silent alarms, and smartphone alarms. These devices generally also require an alarm panel, which detects the duress signal and triggers further action. Table 4-13 displays examples of each.

Note: Alarms should not be confused with sirens. Alarms create an alert, indicating the presence of an intruder, whereas sirens create a sound when activated.

Another device that operates like an alarm is an emergency call box. Emergency call boxes are a form of two-way communications and are further discussed in Subsection 5.2.3.

Table 4-13 Examples of Alarm Types

Alarm Type	Description	Example
Alarm panel	These devices are electrical boxes, often mounted to a wall, that contain connections to different sensors and alarms. The alarm panel gathers input from alarms or sensors and generates alerts according to the situation.	 60
Badge alarm	These devices are worn by school staff (or in some cases, students). Many are worn around the neck. The badge alarm has a button that, when pushed, will signal an alert to an alarm panel.	 61
Panic button	These devices are physical buttons or levers that are openly displayed in common areas for individuals to activate in emergency situations. When triggered, the panic button signals an alert to an alarm panel.	 62
Silent alarm	These devices are buttons or switches are discreetly located within reach of selected school staff to secretly activate in emergencies. When triggered, the silent alarm signals an alert to an alarm panel.	 63
Smartphone alarm	These are applications that run on mobile smart devices. (Smart devices can also include mobile tablets.) These applications run on the phone's native operating system and can be made readily available through an application marketplace.	 64

⁶⁰ <http://www.patent.com.sg/product-details.php?catid=10&subcatid=17&prodid=39>

⁶¹ <http://www.ekahau.com/real-time-location-system/blog/tag/panic-button/>

⁶² <http://alertus.com/capabilities/panicbutton>

⁶³ <http://www.unitedsecurity.com/images/product-images-large/hold-up/HUB2B-ES.jpg>

⁶⁴ <http://techcrunch.com/2012/06/26/clever-bsafe-panic-alarm-app-launches-in-us-with-free-offer-to-new-yorkers/>

4.4.2 HOW THE TECHNOLOGY IS USED

Duress alarms are used to communicate the presence of an individual or condition that is undesirable in the school environment. While a duress alarm could be used to communicate that a medical emergency is occurring, the focus of this report is criminal acts of violence. Therefore, the discussion is limited to this scenario. Duress alarms are triggered when an individual in the school such as a teacher, administrator, or student notices the presence of something or someone that causes him or her to activate the duress alarm. Following its activation, an alert warns of the potential presence of an individual with criminal intent.

Figure 4-11 shows the process for a human-triggered alarm.

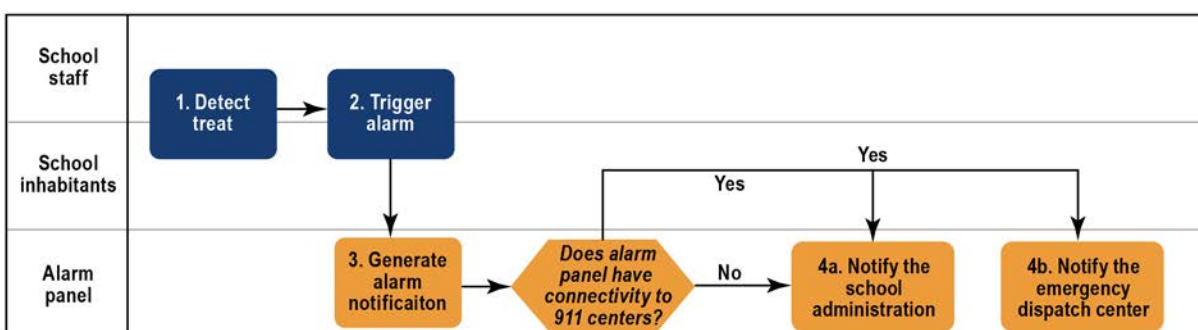


Figure 4-11 Process for Human-Triggered Alarms

Once an intruder is detected by a school student or school staff (step 1), the duress alarm (step 2) is triggered. An alarm notification is sent to the alarm panel to be processed. Once the alarm is triggered, a signal is sent to the alarm panel for processing. Subsequently, the alarm panel generates an alert notification, by way of lights, sounds, sirens, or other devices (step 3). Depending on its configuration, the alarm panel can send a notification to school officials (step 4a), a 911 emergency dispatch center (step 4b), or both.

Different duress alarms types are mounted in different configurations. For example, panic buttons are usually mounted to a wall. This allows the panic button to be highly visible and easily accessible. Panic buttons are intended for use by anyone in distress. Badge alarms have no permanent mount. Instead, these devices are worn on the body, frequently around the neck. Like panic buttons, badge alarms are also highly accessible and highly visible devices. The cost of purchasing badge alarms may limit how many badge alarms a school can purchase. As a result, school staff may be the only persons to wear badge alarms.

Silent alarms are the most discreet type of duress alarm. These devices are mounted in hidden locations, such as underneath desks in the school office. Hiding the location of silent alarms is intentional. A silent alarm may not help with deterring or preventing an intruder, but it can drastically reduce the police response time by triggering a quick alarm. Like badge alarms, silent alarms are intended for use by school staff.

Smartphone alarms are software applications that run on mobile smart devices. The advantage to using this method of duress alarm is that schools can acquire and manage the duress alarm software license without having to worry about acquiring and installing individual duress alarm devices. The school can leverage the smart devices of the school occupants (i.e., teachers, students, and staff). The disadvantage

is that not all environments will have a majority population of smart device users, nor the coverage required. In addition, elementary and middle school students may be less likely than high school students to carry smart devices.

4.4.3 WHAT MAKES THE TECHNOLOGY GOOD?

4.4.3.1 How the Technology Works

When activated, duress alarms send a signal (either through a wire or wirelessly) to the alarm panel. The alarm panel recognizes the signal and triggers an alert or sends a notification to a predetermined list of individuals. This may depend on the design of the duress alarm and alarm panel and/or the policies stated in the school's emergency response plan.

"There are generally three types of information that duress alarms can generate:

- **Panic-button alarm:** A pushbutton mounted in a fixed location. It sends information that there is an emergency situation, and possibly the room in which the panic button is located.
- **Identification alarm:** A portable badge alarm device can identify the person using the duress alarm.
- **Identification and location alarm:** A portable device that identifies, locates, and tracks the person who activated the duress alarm."⁶⁵

4.4.3.2 Differentiators

Duress alarms are fairly simple devices that generate an alert when a button is pressed. However, there are two contributing factors one should consider when comparing performance between vendors:

- **Relevant information:** Some devices can provide a variety of information such as who initiated the alarm, when it was initiated, where the alarm was initiated, and the type of emergency (e.g., a security emergency versus a fire emergency).
- **Ease of use:** Some devices feature a single button that will trigger a response for any emergency. More sophisticated devices use multiple buttons that correspond to various types of emergency situations.

4.4.3.3 Specifications and Features

Table 4-14 presents a range of specifications for duress alarms. The specifications provide specific metrics for comparing different types of duress alarms.

⁶⁵ <https://www.ncjrs.gov/school/ch5.html>

Table 4-14 Technical Specifications for Duress Alarms

Dimensions (Panic Button)	
Length	2.9 to 3.0 in (74 to 76 mm) ^{66, 67}
Width	0.90 to 1.81 in (23 to 46 mm) ^{68, 67}
Height	0.45 to 1.0 in (11 to 25 mm) ^{68, 67}
Dimensions (Badge Alarm)	
Length	2.2 to 3.54 in (56 to 90 mm) ^{69, 70}
Width	1.25 to 2.36 in (32 to 60 mm) ^{71, 70}
Height	0.33 to 0.75 in (8.5 to 19 mm) ^{70, 72}
Dimensions (Silent Alarm)	
Length	2.43 to 3.5 in (62 to 89 mm) ^{73, 74}
Width	1.25 to 2.26 in (56 to 57 mm) ^{75, 73}
Height	0.79 to 1.25 in (20 to 32 mm) ^{76, 74}
Power Supply (Panic Button)	
Wired	Powered by alarm panel
Wireless	12 VDC battery (life up to 2 years) ⁶⁷
Power Supply (Badge Alarm)	
Wireless	1.5 to 3.5 VDC battery (life up to 3 years) ^{77, 72}
Power Supply (Silent Alarm)	
Wired	Powered by alarm panel
Wireless	None
Connections	
Wired	Alarm panel
Wireless (radio)	Alarm panel
Wireless (IP)	Alarm panel, IP-based devices
Specifications (Panic Button)	
Operating temperature	0 to 100 °F (–17 to 37 °C) ⁸⁶
Transmission distance	450 ft (137 m) ⁶⁷

⁶⁶ http://www.utcssecurityproductspages.eu/ED/products_single.php?product=3045-W

⁶⁷ http://www.globalindustrial.com/p/safety/security/surveillance-systems/add-on-wireless-panic-button-for-air-alarm-series?infoParam.campaignId=T9F&gclid=COvcg7fc_scCFQyPHwodNjMPMA

⁶⁸ http://www.ntepartsdirect.com/ENG/PRODUCT/54-634?gclid=CKz6pdXm_scCFdgJgQod6YYGIw

⁶⁹ <http://www.inovonics.com/product/double-button-water-resistant-pendant-transmitter/>

⁷⁰ <http://www.ekahau.com/real-time-location-system/technology/wi-fi-tags>

⁷¹ <http://www.dsc.com/index.php?n=products&o=view&id=110>

⁷² http://www.interlogix.com/_assets/library/78412_wireless_sensors_bro_web.pdf

⁷³ <http://www.unitedsecurity.com/pages/holdup.html>

⁷⁴ <http://www.security.honeywell.com/hsc/products/intruder-detection-systems/sensor/hold-up-switch/21638.html>

⁷⁵ <http://www.seco-larm.com/Double.htm>

⁷⁶ <https://www.vikingelectronics.com/product-details.php?pid=332>

⁷⁷ <http://www.napcosecurity.com/keyfobs.html>

Table 4-14 Technical Specifications for Duress Alarms (Continued)

Specifications (Badge Alarm)	
Operating temperature	32 to 140 °F (0 to 60 °C) ⁶⁹
Transmission distance	140 to 1000 ft (40 to 304 m) ^{70, 72}
Specifications (Silent Alarm)	
Operating temperature	14 to 140 °F (–10 to 60 °C) ⁷⁴
Specifications (Alarm Panel)	
Operating temperature	–4 to 131 °F (–20 to 55 °C) ^{78, 79}
Zones	4 to 32 ^{80, 81}
Zone types	2 to 4 ^{82, 83}
User codes	8 to 48 ^{84, 85}
Features (Panic Button)	
Visual indicator that unit has been activated. ⁸⁶	
Features (Badge Alarm)	
Multiple call buttons ⁷⁰ Customizable alarms ⁷⁰ Indicator (visual or otherwise) to indicate signal transmission ⁷¹ Recessed panic button provides greater immunity from false alarms ⁷² Small design can be worn discreetly ⁷² Mechanism to eliminate accidental triggering ⁷²	
Features (Silent Alarm)	
Silent actuating button ⁷³ Compact size ⁷⁵ Mechanism to eliminate accidental triggering ⁸⁷ Tamper protected switch mechanism ⁸⁷ Ability to mount at any angle ⁷⁶	

⁷⁸ http://www.nortekcontrol.com/product_detail.php?productId=1561⁷⁹ <http://heimen.manufacturer.globalsources.com/si/6008825081915/pdtl/Fire-alarm/1131366022/Security-Alarm-Control-Panel.htm>⁸⁰ http://www.interlogix.com/_/assets/library/73841_network_cp_data.pdf⁸¹ <http://www.dsc.com/index.php?n=products&o=view&id=53>⁸² <http://www.security.honeywell.com/hsc/products/intruder-detection-systems/control-panel/burglary/ademco-vista/14957.html>⁸³ <http://www.security.honeywell.com/hsc/products/intruder-detection-systems/control-panel/burglary/ademco-vista/14958.html>⁸⁴ http://www.interlogix.com/_/assets/library/73841_network_cp_data.pdf⁸⁵ https://www.jmac.com/Honeywell_Ademco_V20P60PK_p/HONEYWELL-V20P60PK.htm?gclid=CLndgf_fzsgCFckWHwodiPoK-A⁸⁶ http://www.utcssecurityproductspages.eu/ED/products_single.php?product=3045-W⁸⁷ http://www.pottersignal.com/product/datasheet/8880126_husd15blbm.pdf

Table 4-14 Technical Specifications for Duress Alarms (Continued)

Features (Alarm Panel)
Can set various programming ⁸⁸
With remote control function, can connect external siren, remote monitor on-site alarm, trigger on-site siren ⁸⁹
Arm/disarm each zone ⁹⁰
Record recent alarm event information, can check at any time ⁹¹
AC power failure, low battery, dropped calls and other fault alarm ⁹²
Early open/late close reporting ⁹³
Wall and case tamper ⁹⁴
24-hour battery backup ⁹⁵

4.4.3.4 Effectiveness

If programmed to automatically notify first responders when activated, duress alarms can streamline an emergency response to potential intruders. When receiving calls, dispatchers usually require time to collect information regarding the nature of the emergency. However, duress alarms can also instantly trigger the need for immediate help to a specific location. Duress alarms, when used discreetly, can notify law enforcement without alerting the intruder of the active response to the incident.

4.4.3.5 Policy Impacts

Schools installing duress alarms should include the location and usage of the alarms in their emergency response plan. For discreet duress alarms, such as the silent alarms, schools do not want to advertise the location of alarms because it would defeat the purpose of the device being discreet. Schools also should incorporate backup emergency plans for when the alarm systems are down or not working as intended.

Schools can also establish a direct connection wherein the alarm goes directly to local law enforcement. However, this must be carefully planned and requires effective policies. Schools trust law enforcement will quickly respond when an alarm is triggered; but schools must be careful to minimize the number of false alarms. Schools may be subject to service fees or penalties if responders are called to excessive false alarms.

⁸⁸ <http://heimen.manufacturer.globalsources.com/si/6008825081915/pdtl/Fire-alarm/1131366022/Security-Alarm-Control-Panel.htm>

⁸⁹ Ibid

⁹⁰ Ibid

⁹¹ Ibid

⁹² Ibid

⁹³ <http://www.interlogix.com/intrusion/product/networkx/>

⁹⁴ <http://www.dsc.com/index.php?n=products&o=view&id=53>

⁹⁵ Ibid

4.4.4 CONCERNS ABOUT THE TECHNOLOGY

4.4.4.1 What It Does Not Do

Duress alarms cannot prevent violence. They also cannot actually protect someone from being victimized, but the ability to rapidly summon assistance when a fight seems imminent or to initiate a lockdown does offer the potential to protect people from violence. However, the effectiveness is critically linked to the ability of an alarm to promptly notify the appropriate people.

One of the limitations to duress alarms is that they may not indicate the type of emergency. Alarms triggered for safety emergencies may require response from firefighters and emergency medical technicians (EMTs). Alarms triggered for security emergencies may require response from police officers and special weapons and tactics (SWAT) team members, as well as the firefighters and EMTs.

4.4.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Regardless of whether the intent is to create an alert discreetly or overtly, the school must be strategic about placing these alarms in areas that can be accessed during routine operations so that staff are not forced to put themselves into additional danger to activate an alarm.

If the location of duress alarm buttons is widely known, intruders can use this information to prevent staff from triggering the alarm. Thus, schools often withhold information about the presence of silent alarms.

4.4.4.3 Possibilities for Misuse

There are ways to misuse duress alarms and cause false alarms. One of the more common misuses is a mischievous child deciding to trigger a duress alarm as a prank. Schools may need to implement disciplinary actions for persons who intentionally trigger a false alarm.

4.4.4.4 Liability and Safety Concerns

False usage of alarms causes concern with the relationship between school officials and law enforcement. As previously discussed, this is a trust relationship in which school officials trust in a quick response from law enforcement and law enforcement trusts the school to minimize or eliminate false alarms. Schools must find ways to mitigate false alarms to eliminate the possibility of not receiving a response when the alarm is triggered.

4.4.4.5 Privacy Concerns

Some badge alarms are being designed using radio frequency identification (RFID) technology. The built-in RFID tag broadcasts the location of the badge alarm. With this tracking capability, schools may encounter privacy issues.

4.4.4.6 Accommodations Needed for Disabilities

All duress alarms must be accessible to people with disabilities. For example, mounted alarms should be placed within reach of someone in a wheelchair, and badge alarms should not require fine motor skills or the use of two hands.

4.4.4.7 Policy Concerns

Schools should establish policies and procedures for appropriate usage of duress alarms. The policy should incorporate where duress alarms are located, who should use them, who is notified (school administration and/or emergency dispatch), and how the school manages the response to a duress alarm. Because triggering a duress alarm may notify police, schools may need to coordinate their policy with the policies of local law enforcement. School policies may also need to address false alarms (i.e., alarm accidentally or mischievously tripped).

4.4.5 COST CONSIDERATIONS

Table 4-15 discusses the various costs that may be associated with duress alarms.

Table 4-15 Duress Alarm Cost Considerations

Cost Factor	Cost Description
Acquisition (Panic Button)	Panic buttons can cost as low as \$7.18 to \$26.32 or as high as \$38.23 to \$72.00. In general, they should cost less than \$100 per unit.
Acquisition (Badge Alarm)	Badge alarms can cost as low as \$31.16 to \$53.49 or as high as \$56.44 to \$75.00. In general, they should cost less than \$100 per unit.
Acquisition (Silent Alarm)	Silent alarms can cost as low as \$6.65 to \$15.00 or as high as \$15.44 to \$30.00. In general, they should cost less than \$50 per unit.
Acquisition (Alarm Panel)	Alarm panels can cost as low as \$101.68 to \$181.20 or as high as \$228.95 to \$578.44.
Installation	“Both hard-wired and wireless panic alarm systems are available. Hard-wired systems are more expensive to install due to the expense of wiring. Future expansion or changes to the system may be expensive because every change means that the system must be re-wired. Wireless systems are a reliable and robust alternative to hard-wired systems. Wireless systems are easier to expand or change as a school’s needs evolve.” ⁹⁶
Operation and labor	Minimal, some types of alarm panels may require monitoring or manual acknowledgement of alarm conditions.
User training	Varies, but generally requires some introduction to the product and intended uses and periodic hands-on drills.
Maintenance	Physical devices (such as badge alarms) may need recharging and minimal routine cleaning per manufacturer’s instructions.
Consumables	Wireless duress alarms require batteries that require periodic replacement. Battery life will vary from vendor to vendor.
Energy and energy dependency	Devices will need to be hardwired (alarm panels) into an electric supply or battery powered (badge alarms).
Software licenses	If duress alarm includes tracking software to identify the location or time of the alarm, then software licenses may be required.
System integration	Varies depending on complexity of integration with other systems, such as video cameras and physical security information management software. Cost may vary with the amount of connectivity from internal (e.g., school security) to external (e.g., law enforcement) notification.

⁹⁶ <http://www.securitymagazine.com/articles/86070-saving-time-and-lives-with-direct-to-responders-alarms>

4.4.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

None identified by the author.

4.4.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 4-16 provides examples of known vendors of duress alarms; however, it is not comprehensive and other vendors may exist. The list is current as of 15 October 2015.

Table 4-16 Duress Alarm Vendors

Vendor	Website	Notes
SecurityMan, Inc.	http://www.securitymaninc.com/	Panic buttons
United Technologies (UTC) (formerly GE Security/Sentrol)	http://www.utc.com/Pages/Home.aspx	Panic buttons
NTE Electronics, Inc.	http://www.nteinc.com/	Panic buttons
iPhone	http://www.iphone.com/	Panic buttons
Ekahau	http://www.ekahau.com/	Badge alarms
Inovonics	http://www.inovonics.com/	Badge alarms
Digital Security Controls	http://www.dsc.com/	Badge alarms
Napco	http://www.napcosecurity.com/	Badge alarms
GE Interlogix	http://www.interlogix.com/	Badge alarms
United Security Products, Inc.	http://www.unitedsecurity.com/	Silent alarms
ADEMCO (a Honeywell Company)	http://www.ademco.eu/	Silent alarms
SECO-LARM USA, Inc.	http://www.seco-larm.com/	Silent alarms
Amseco (a Potter Brand)	http://www.pottersignal.com/	Silent alarms
Viking	https://www.vikingelectronics.com/	Silent alarms

4.5 FURTHER READING

For additional information, consult the following:

- Fennelly, L., and Perry, M. (2014) *The Handbook for School Safety and Security: Best Practices and Procedures*. Butterworth-Heinemann.

4.6 CONCLUSION

This chapter covers a range of alarms and sensors, a collective system of components that operate autonomously to enable the early detection of intruders. Sensors discussed in this chapter include motion sensors and open-door sensors. Alarms covered include panic buttons, badge alarms, silent alarms, and alarm panels. Systems available in many of the alarm and sensor categories discussed are being continually improved as available and/or applicable technologies advance. School officials should carefully consider the capabilities, limitations, costs, policy impacts, and other relevant factors prior to upgrading or installing alarm or sensor systems. They should also carefully consider the potential technological advancement of these systems and, when possible, accommodate current and future

system integration and upgrade possibilities. Many of the technologies discussed can be integrated with access control or other systems (e.g., surveillance systems and cameras) to provide more robust school safety capabilities.

Chapter 5. TECHNOLOGY REVIEW – COMMUNICATIONS

*William R. McDaniel, PhD; Subramaniam Kandaswamy, PhD; Lauren A. Brush, MS; and
Patrick A. Shilts, MS*

5.1 INTRODUCTION

For the purposes of this report, communications technologies are defined as devices designed to facilitate or monitor communications between personnel within the school or between school personnel and stakeholders outside the school such as first responders, administrators, or the surrounding community. Some technologies are intended for one-way communications, while others allow two-way communications. In one-way communications, a message is transmitted or broadcast with no means for acknowledgment or response. With two-way communications, messages may be exchanged between two or more parties.

The following technologies are discussed further in Sections 5.2 and 5.3:

- Two-way communications technology
 - **Two-way radio:** A transceiver device that can transmit as well as receive voice communications.
 - **Intercom or public address (PA) system:** A two-way communication system with a microphone and loudspeaker at each station.
 - **Emergency call box:** A permanently mounted device, often outdoors, that enables voice communications with a person in distress. Because of the device's fixed location, the person's location is known.
 - **Telephone:** A traditional landline or cellular telephone system delivered by a commercial carrier.
- One-way communications technology
 - **Emergency Notification System (ENS):** A system that can simultaneously send information regarding an emergency event through multiple modes, including phone call, text message, smartphone app, email, etc.
 - **Bullhorn:** A handheld voice-amplification device.
 - **Digital sign or billboard:** A message center or board, either streaming text via light-emitting diode (LED) display or pictures and video via flat screen monitor.
 - **Datacasting:** A system, including hardware and software, for sending information over unused portions of television (TV) broadcast channels.

Communication, of course, is necessary for many purposes, but the intent of this chapter is to describe communications technologies as they relate to school safety. The distinction between one-way and two-way communications is relevant to school officials as they consider whether transmitting or receiving information is their district's primary communication need. It also useful to make a distinction based on operations rather than a distinction based on subsets of technology. The same device, for instance a cell phone, may be used for either one-way or two-way communication, depending on what technology is applied.

It is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district prior to purchasing a safety or security technology. Table 5-1 presents the means by which the study team evaluated communications capabilities, aligned with the Federal Emergency Management Agency (FEMA) mission areas: Prevention, Protection, Mitigation, Response and Recovery.¹ This assessment combines the opinion of security subject matter experts and the informed judgment of the authors who evaluated the technologies. Reviewing this table provides a summary of the areas of school security and safety for which communications may be best suited.

Table 5-1 Communications – Technology Impact Summary

Device	Prevention	Protection	Mitigation	Response	Recovery
Two-Way Communications					
Two-way radio	NONE No effect on prevention noted	NONE No effect on protection noted	NONE No effect on mitigation noted	HIGH Can be a primary means of communication during an event.	HIGH Can be used immediately after an emergency for communicating recovery activities

¹ The preparedness cycle consists of the following five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.
- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

Table 5-1 Communications – Technology Impact Summary (Continued)

Device	Prevention	Protection	Mitigation	Response	Recovery
One-Way Communications					
Intercom or PA system	NONE No effect on prevention noted	NONE No effect on protection noted	NONE No effect on mitigation noted.	MEDIUM Only useful to communicate information that responders, perpetrators, and potential victims should all hear	NONE No effect on recovery noted
Emergency call box	LOW Presence might discourage threats	NONE No effect on protection noted	NONE No effect on mitigation noted	MEDIUM Enables responders to locate event; visibility encourages witnesses to call for help	NONE No effect on recovery noted
Telephone	NONE No effect on prevention noted	NONE No effect on protection noted	NONE No effect on mitigation noted	HIGH Universal method for contacting first responders	HIGH Can be used immediately after an emergency for communicating recovery activities
Emergency notification system	NONE No effect on prevention noted	NONE No effect on protection noted	NONE No effect on mitigation noted	LOW Enables school officials and law enforcement to deliver information and directions during an active incident	MEDIUM Communicating messages to parents can greatly reduce their anxiety and reduce the volume of calls from parents and other concerned citizens
Bullhorn	NONE No effect on prevention noted	NONE No effect on protection noted	NONE No effect on mitigation noted	LOW Standalone communication not dependent on external power or networks	LOW May be used during reunification efforts

Table 5-1 Communications – Technology Impact Summary (Continued)

Device	Prevention	Protection	Mitigation	Response	Recovery
Digital sign or billboard	NONE No effect on prevention noted	NONE No effect on protection noted	NONE No effect on mitigation noted	LOW Enables school officials and law enforcement to deliver information and directions during an incident	LOW Can communicate outcomes and changes to plans to school staff and students
Datacasting system	NONE No effect on prevention noted	NONE No effect on protection noted	NONE No effect on mitigation noted	LOW May enable communication when Internet and cellular systems are overloaded	LOW May be used to distribute maps, blueprints, attendance lists, etc. to assist reunification and recovery efforts
<p>Impacts as they relate to a technology's ability to impact a school's ability to <i>prevent, protect, mitigate, respond, or recover</i> from an incident.</p> <p>High: Technology is expected to have a <i>significant</i> impact.</p> <p>Medium: Technology is expected to have <i>some</i> impact.</p> <p>Low: Technology is expected to have <i>little</i> impact.</p> <p>None: Technology is expected to have <i>no</i> impact.</p> <p>Caution: Technology will have an impact; however, it may also have unintended consequences.</p>					

For school safety purposes, communications technologies are most important during and after an event. As with other technologies, integrating communications with the overall school safety plan increases the effectiveness of these technologies across all areas. Communications technologies are discussed in greater detail in Sections 5.2 and 5.3.

5.2 TWO-WAY COMMUNICATIONS

5.2.1 TWO-WAY RADIOS

5.2.1.1 Introduction

Radios have been used in schools for a number of years for communications between teachers, administrators, emergency responders, and security staff during routine and emergency situations.

Unlike a cellphone which uses two different radio frequencies to enable full-duplex mode where enabling one to talk and listen at the same time, a two-way radio (Figure 5-1) is a transceiver that operates in half-duplex mode, allowing a user to send (talk) or receive (listen) communications, but not both at the same time. A two-way radio allows a user to communicate with others using similar radios operating in the same frequency and relative location.



Figure 5-1 Examples of Two-way Radios

Three broad categories classify two-way radios: the physical form, the signal type (analog or digital), and the radio spectrum used. Each physical form has accessories, such as chargers or antennas to improve performance or ease of use.

5.2.1.1.1 Form

Two-way radios are available in three basic forms: handheld portable, vehicle-mounted mobile, and desktop base station. Handheld radios are small, lightweight, portable, and battery powered. Vehicle-mounted radios are mounted in a car or truck and draw their power from the vehicle's battery. Their range is boosted using an externally mounted antenna rather than one on the radio set. Vehicle-mounted radios can also be used as mobile base stations. Desktop base stations are installed in fixed locations and draw on external power [e.g., alternating current (AC) or direct current (DC)], and are used for communication between a dispatch or command center and mobile or portable radios in the field. They often have externally mounted antennas, depending on their intended use and expected signal reach. Some base stations also include charging ports for handheld radios used by mobile users.

5.2.1.1.2 Analog and Digital Radios

Analog radios transmit an analog signal over the air after modulating and amplifying it. Analog signals assume the continuous sinusoidal form of the radio waves over which they ride. Analog radios are simple, inexpensive, and robust. However, analog signal quality degrades more at extended ranges and limits the user to one conversation at a time per analog channel.

Digital radios transmit digitized signals after converting the original analog content into binary digits. In comparison to analog, digital radios offer better voice quality, many more features, and better security. They also support Internet Protocol (IP) connectivity, which allows transmission or receipt of emails and text messaging to non-radio users as well, and many are equipped with global positioning system (GPS) technology. On the other hand, digital radios are more complex and more expensive to purchase and maintain than analog radios.

5.2.1.1.3 Radio Spectrum

Common two-way radio systems operate in the very high frequency (VHF), ultra-high frequency (UHF), and 700- to 800-MHz parts of the radio spectrum. Frequency refers to the rate of peaks in the radio wave, with a higher number indicating more wave peaks per second, as measured in hertz (Hz) or, more commonly for radio signals, megahertz (MHz). Transmitters are tuned to send the radio signal at a certain frequency so that receivers tuned to the same frequency receive that signal.

- **UHF radio:** Commercial UHF radios operate in the radio spectrum between 400 and 512 MHz. The UHF radio frequency is used for two-way radios, GPS, Bluetooth, cordless phones, and Wireless Fidelity (WiFi). Interference caused by electrical equipment is lower in the UHF band.
- **VHF radio:** Commercial VHF radios operate in the radio spectrum between 130 and 174 MHz. VHF waves travel farther than UHF waves, which makes VHF more effective when broadcasting over a long range.
- **700- to 800-MHz radios:** Public safety officials, such as police and fire departments, generally use radios operating between 700 to 800 MHz. These types of radios are suited for indoor applications and areas with obstructions (e.g., concrete walls). They are also used for trunking two-way radio systems—the practice of sharing a limited number of communication channels (trunks) among many users.

In summary, VHF and UHF bands are typically used for conventional two-way radio systems. For inside school buildings, UHF radios usually have less interference, and for outdoor use, VHF radios are more desirable.

5.2.1.1.4 Radio Equipment Accessories

There are many common accessories that enhance the user experience for two-way radios, including headsets (wired or wireless), carrying cases, batteries and chargers, and speakers. Because analog technology has been in use longer, there is a perception that more accessories are available for these types of radios. However, digital radios allow for a much wider variety of features, especially through software, and may have a wider variety of relevant accessories depending on the application.²

Some users will also install repeaters to supplement two-way radios. A repeater receives transmissions from portable two-way radios and then rebroadcasts them at a much higher wattage on a different frequency, thereby providing a much larger coverage area.

5.2.1.2 How the Technology Is Used

Two-way radios provide a reliable method of communication between rooms and buildings at a single site or separate sites. Typical users include the principal, administrative assistant, security staff, police, school bus drivers, public safety staff, maintenance and operation staff, food service and cafeteria workers, and athletic directors. Teaching staff may or may not be assigned radios.

According to a 2013 survey,³ the top five school staff positions that rely on two-way radios are:

- Principals (70%)
- Maintenance workers (65%)

² <http://bearcom.com/wp-content/uploads/BearComAnalogVsDigitalWhitePaper.pdf>

³ Motorola, 2013 Nationwide Survey, White Paper, K-12 Education Communications

- School bus drivers (64%)
- Administrators (58%)
- Security officers (46%)

Per the same survey, the top five places where two-way radios are used are:

- Bus and student loading zones
- After-school programs
- Fields and playgrounds
- Assemblies and sporting events
- Field trips

During local and regional emergencies, landline and cellular telephone networks can easily become inundated with calls and this traffic volume can prevent or hamper communication. Radios on a private IP-based network can accommodate time-sensitive communication during these times of peak telephone network congestion. Patrol cars, ambulances, and fire engines equipped with compatible two-way radios can potentially enable seamless communication between the first responders and the school and/or school system. Public safety two-way radio systems operate on exclusive and different frequencies, but software exists to provide interoperability between these systems and school radio systems. Although these technologies allow emergency personnel to interconnect across systems, they are usually not controlled by school systems and therefore are not considered in this review. However, some states, such as New Jersey, “... recommend that the State require, either through legislation or regulatory measures, school districts to provide two-way radios that have the capability for a dedicated channel, separate from regular operational police frequencies, to enable all school security personnel to communicate directly with other emergency responders.”⁴

The National Center for Educational Statistics (NCES) provides statistics on “two-way radios provided to staff” for public schools (Reference 353). It is estimated that about 74% of all public schools have provided these radios to their staff. Use is less prevalent in high schools—only 65% of which provide radios—than in middle and elementary schools. Also, smaller schools and rural schools are less likely to provide radios for staff, whereas larger schools and city or suburban schools are more likely; for example 84% of suburban schools provide radios.

Schools use two-way radios for emergencies as well as managing their everyday needs. Some examples include classroom communication between administrators and school security staff, in bus and student loading zones, during field trips and sporting events, and while managing after-school programs.

With two-way radios, “All I have to do is push the transmit button to speak to anyone at our schools or our alternative locations either privately or as a whole broadcast,” says Joye Fuston, CLA, administrative assistant, Warren County Schools. “If a crisis occurs at any of our locations, personnel can send me an emergency transmission, and I can monitor the situation without the trespasser even being aware; therefore allowing me the opportunity to contact 911. Our system-wide SRO [School Resource Officer] is also able to hear each transmission and can respond immediately upon hearing of a situation.”⁵

⁴ New Jersey School Security Task Force Report and Recommendations, July 2015.

⁵ www.campussafetymagazine.com/article/Two-Way-Radios-Keep-K-12-Campuses-Connected

5.2.1.3 What Makes the Technology Good?

5.2.1.3.1 Differentiators

Two-way radios may be preferred over phones because they can operate anywhere within the signal reach without relying on a telephone network. They also offer instant communication and facilitate group communication (single-point to multi-point). Radios consume little power, require no service fee, and most provide a capability to send a duress call during emergencies. Some radios with GPS tracking capabilities enable tracking of radio location, such as on school buses, for security reasons.

5.2.1.3.2 Specifications and Features

Radios are built to use either an analog or digital signal. Digital is preferable but currently a more expensive option than analog. Two-way digital radios with dual- or mixed-mode operations are capable of operating in either analog or digital mode and permit backward compatibility with legacy analog units. This allows legacy radios to be phased out slowly as funds become available. Digital radios may also include tamper alarms to indicate improper use of the signal and may include cyber-security features.

Radio signal coverage area is a function of power. Range claims made by vendors are based on optimal conditions (e.g., having an unobstructed line of sight between the source and the destination and a high vantage point in good weather conditions). In 90% of cases, the actual range is 2 miles or less,⁶ once users account for topography (e.g., hills), weather (e.g., thick clouds), obstructions (e.g., dense forest or tall buildings), large metal surfaces, and other limiting factors. However, repeaters can extend the range. UHF frequencies should be chosen if radios are intended for indoor use, where the communications will be less affected by obstructions. Because of their larger range, VHF bands should be chosen if radios are intended for outdoor use.

Radio signals travel over channels in their frequency range, and the number of channels a radio accommodates dictates the number of separate communications that can take place in the same coverage area. Most radios offer one to two dozen channels and up to 121 privacy (or interference-elimination) codes for each main channel. Some vendors offer 128 or more channels.⁷ All radios should communicate with each other and with base stations. Interoperability with emergency response radio systems can be achieved if responders have dual-band radios; however, before making a purchase decision, school officials should coordinate with police and fire departments to determine whether they have such radios and, if so, what bands are available for communications.

One accessory of particular importance is the repeater. A repeater receives transmissions from portable two-way radios and then rebroadcasts them at a much higher wattage, providing a much larger coverage area. By some estimates, range for UHF radios can increase from a half mile to as much as 25 miles (outdoors).⁸

The battery or radio is usually charged using a basic AC rapid charger unit. Battery life is highly dependent on the make and model of the radio and its intended use. No special dedicated staff or specialized knowledge is required for operating most radios. Procedures must be established and personnel trained regarding the operational use of radios, but this training is not directly related to the

⁶ <http://www.rei.com/learn/expert-advice/twoway-radios.html>

⁷ <http://www.buystwowayradios.com/cat/2-way-radios/guide/business/use/schools.aspx>

⁸ <http://www.bridgecomsystems.com/blogs/bridgecom-tx-rx-blog/18728421-repeater-basics-what-is-a-2-way-radio-repeater-and-how-is-it-used>

technology. Some radios permit operations without pushing any button so that users who are disabled or temporarily unable to move can still communicate.

5.2.1.3.3 *Effectiveness*

Although NCES offers statistics on the percentage of school staff provided with two-way radios, no statistics on the effectiveness of the technology are available. Performance factors for evaluating two-way radios include durability, battery life, flexibility and practicality, and security.

- **Durability:** Most vendor products are built to withstand rough handling. There are also water-resistant and waterproof models for many radios.
- **Battery life:** Two-way radio batteries are designed to hold enough charge to comfortably last through a 12-hour shift when fully charged. Most batteries are expected to be replaced after 18 to 24 months of continuous use, but this depends on proper maintenance.⁹
- **Flexibility and practicality:** At the push of a button, two-way radios allow individuals to communicate with large groups of radio users.
- **Security:** Some two-way radios use private networks with privacy and encryption options.

5.2.1.3.4 *Requirements*

An important aspect of the technology is the switch to narrow-banding mandated by the Federal Communications Commission (FCC)¹⁰ in December 2004 to increase the available spectrum in the VHF and UHF private land mobile bands. Most legacy radio systems operate on wideband channels of 25 kHz. The width of the channel indicates the range of frequencies associated with that channel. A radio assigned to a channel may broadcast at any frequency in that range, but usually aims for the center of the range. Better radios are able to keep their signal well within the frequency bounds. Newer technologies, usually but not necessarily associated with digital signals, can operate without interference in narrower channels. The FCC cuts these channels in half to 12.5 kHz, thus doubling the number of frequencies under the narrow-banding policy. This is necessary because many more devices and systems use radio waves as part of their operations, resulting in existing channels getting “crowded” by too much traffic passing over them, which diminishes the quality of the signal.¹¹ The FCC target date for this conversion was 1 January 2013, meaning any equipment not capable of operating on channels of 12.5 kHz or less need to be replaced. However, the implementation of this policy is incomplete. Radio systems still using wideband channels beyond the target date risk loss of radio communications, fines imposed by the FCC, revocation of license, and/or interference issues.

5.2.1.3.5 *Policy Impacts*

School districts should establish policies on the appropriate use of two-way radios for communications and integrate this with their policy on the use of phones, intercoms, and other communication devices.

When developing or updating emergency operating plans, school districts should work with all segments of the community emergency response team and develop a joint plan of action on the use the two-way radio technology during emergencies. This includes coordinating radio frequency use with police, fire, security, and medical personnel and with other radio users. The school should identify radio coverage

⁹ http://www.motorolasolutions.com/content/dam/msi/docs/en-xw/static_files/IMPRES_Madison_Case_Study.pdf (accessed 29 December 2015)

¹⁰ https://transition.fcc.gov/pshs/docs/clearinghouse/guidelines/Narrowbanding_Booklet.pdf

¹¹ https://transition.fcc.gov/pshs/docs/clearinghouse/guidelines/Narrowbanding_Booklet.pdf

needs and potential weak spots in a building (e.g., where radio signals cannot penetrate) and develop mitigation plans. Step-by-step directions containing operational instructions and procedures for radio use should be documented. Simulating emergency conditions and rehearsing procedures will help identify process and procedural gaps as well as execution difficulties.

5.2.1.4 Concerns About the Technology

5.2.1.4.1 General Discussion (What It Does Not Do)

Unlike telephone networks that are not bound by distance, radios without repeaters are limited in range, especially in the presence of obstructions such as trees, hills, or buildings. These obstructions can block the signal and dramatically reduce the range of a two-way radio.

5.2.1.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Two-way radio communications may be intercepted by unintended recipients, so appropriate security measures should be taken. School districts must also plan for maintenance and replacement costs, especially when considering integration with emergency response personnel.

5.2.1.4.3 Possibilities for Misuse

Although the likelihood of occurrence is low, two-way radios in the wrong hands can result in pranks or malicious acts. Radios operating without encryption are also susceptible to interception of signal, enabling third parties to listen in on the communications without being detected.

5.2.1.4.4 Liability and Safety Concerns

None identified by the authors.

5.2.1.4.5 Privacy Concerns

None identified beyond those associated with signal interception.

5.2.1.4.6 Accommodations Needed for Disabilities

Americans with Disabilities Act (ADA) compliance is only applicable to the staff who are assigned two-way radios to communicate. There are radios on the market that are activated by voice.

5.2.1.4.7 Policy Concerns

None identified, but radio use should be addressed in the school safety plan.

5.2.1.5 Cost Considerations

Digital radios are more expensive than analog radios, but in general two-way radios offer a cost-effective solution compared to expensive intercom systems. The cost of radios can vary based on a number of factors. The number of accessories such as repeaters and support for features such as GPS tracking will increase the cost. For the latter, there may be subscription and other costs. Some cost factors to consider are described in Table 5-2.

Table 5-2 Radio Cost Considerations

Cost Factor	Cost Description
Acquisition	Radios generally come with batteries and chargers. Some systems incorporate chargers with base stations. The number and types of base stations will also affect cost. Depending on use, antennas and towers may be needed. Holsters, headphones, and other accessories may also be purchased.
Installation	Schools must install or lease towers and base stations.
Operation and labor	None
User training	Minimal
Maintenance	Radios require little maintenance, but are prone to damage in typical work environments. Replacement cost, likely similar to acquisition cost, should be accounted for.
Consumables	New batteries approximately replaced every 1.5 years. Some radios can only use original equipment manufacturer (OEM) batteries.
Energy and energy dependency	Battery power, AC power for the charger.
Software licenses	Not applicable (N/A)
System integration	Software and hardware are available to provide interoperable communications with other communication systems.

5.2.1.6 Emerging Technologies and Future Considerations

The FCC proposes that all radios be digital by 2018.¹² Although it is not yet a mandate and the date is subject to change, the obvious implication for schools is to carefully consider avoiding the purchase of analog radios. However, because digital radios are more expensive than analog radios, budget could be a limiting factor.

5.2.1.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 5-3 presents examples of known vendors of two-way radios; however, it is not comprehensive and other vendors may exist. Most of these vendors supply a wide variety of radios, so school officials should consider what features are of most importance in their districts. The list is current as of 13 October 2015.

¹² https://transition.fcc.gov/pshs/docs/clearinghouse/guidelines/Narrowbanding_Booklet.pdf

Table 5-3 Two-Way Radios Vendors

Vendor	Website
Bear.com	http://bearcom.com
Cobra	https://www.cobra.com/
ESS	http://essnashville.com/products/motorola-two-way-radios/
Icom	www.icomamerica.com
Harris	http://harrisradio.com/product-family/portable/
Kenwood	www.kenwoodusa.com
Midland	https://midlandusa.com/two-way-radios
Motorola	http://www.motorolasolutions.com/en_xu/products/two-way-radios-licensed/portable-radios/cp-commercial-series.html
TwoWayDirect	http://www.twowaydirect.com
Uniden	https://www.uniden.com/two-way-radios

5.2.1.8 Further Reading

Additional resources to consider are:

- “2-Way Radio Range: How Far Can Two-Way Radios Communicate?”
<https://www.intercomsonline.com/Articles.asp?ID=308>
- “User Equipment General Deficiencies,” San Rafael (CA) Police Radio Committee Report to the Mayor and City Council, 1995, pp. 12.

5.2.2 INTERCOMS AND PUBLIC ADDRESS SYSTEMS

An intercom is a two-way communication system, whereas a PA system supports one-way communication. They are both single-point to multi-point communication devices used to transmit information quickly to a wide audience. Intercoms can also connect to a PA system. The focus of this subsection is two-way intercoms.

5.2.2.1 Introduction

The school intercom (Figure 5-2) is a simple and effective method of internal communication. An intercom is a voice communication system used within a building or a small collection of buildings operating on its own network, often hardwired. Intercoms are customarily mounted permanently on the wall, but may also be mounted in vehicles. Many models can support connections to public address loudspeaker systems, handheld radios, telephones, and other intercom systems. A few provide control of devices such as signal lights and door latches.



Figure 5-2 Example of an Intercom¹³

Although not primarily considered a school safety technology, intercoms can play an important role in emergency situations. For instance, the Sandy Hook Advisory Commission report (Reference 297), in the section titled, “Key Safe School Infrastructure Council Standards,” recommends:

“4.12 Call buttons with direct intercom communication to the central administrative office and/or security office should be installed at key public contact areas.

5.24 Control visitor access through electronic surveillance with intercom audio and remote lock release capability at the visitor entrance.”

These two uses are both relevant but somewhat distinct because the intercom associated with an access control system (for more information about this application, see Chapter 3) usually operates on a separate network that primarily supports access control. This subsection focuses on intercom systems commonly associated with classrooms, but will point out relevant features associated with access-control intercoms.

5.2.2.1.1 Components of an Intercom

Basic components of an intercom include:

- **Base station:** Usually located in the main office of a school, the base station controls the intercom system and can initiate communication with individual substations or can broadcast announcements over them. The base station can also receive calls from substations and precisely indicate where the call is coming from (e.g., “4th grade, Mrs. Jones’s classroom”).

¹³ <http://www.aiphone.com/home/markets/educational/>

Many systems have a capability that allows school staff to call the base station and either record a message or pick from a set of prerecorded messages to broadcast to all substations.

- **Substations:** Located in classrooms, gyms, libraries, and other areas where students and staff congregate, substations receive messages broadcast from the base station. Substations can also communicate one-on-one with the base station through calls that can be initiated by either the base station or the substations, but substations cannot initiate calls to other substations.
- **Door station:** Located at the primary visitor entrance(s), these stations may function through an access control system or send calls to the intercom base station. Depending on the access control system, they may or may not have a video unit.

5.2.2.1.2 *Types of Intercoms*

There are several variations on intercom operation and installation. For voice communication, the most basic form is the simplex intercom system. In this type of intercom, communications occur in only one direction, so a user can either speak or listen at a given time but not do both. With a duplex intercom system, communications can occur in both directions, allowing a user to speak and listen at the same time, similar to a telephone call.

Some intercoms use a handset, similar to a landline phone, at the base station and substations. These systems maintain acceptable voice quality even in a noisy environment and offer some degree of privacy, but limit the mobility of the user. With a hands-free intercom, base stations and substations incorporate a speaker and microphone in the unit. Hands-free intercoms allow more mobility, but they offer little privacy and are hard to use in a noisy environment. Some units have both features, with the mode controlled by the user in case a private conversation needs to take place.

The longest-lived installation method is a wired intercom system. This type of intercom requires hard wiring between the base station and each of the substations. They are costly to install, but are very reliable and require less maintenance than wireless installations. Especially following the FCC's rule change regarding multi-use radio services in 1992,¹⁴ vendors also offer intercom systems that use wireless signals to link base stations with substations. No wiring is needed, and units are much easier to install. However, concrete walls and steel frames can block the signal, resulting in performance degradation as the physical distance between the source and the destination increases. There are also IP-based intercom systems that can interface with the school's existing data networks by plugging into a nearby network outlet or unused port. This can significantly reduce the cost of installation and maintenance because IP-based base stations and substations can be more easily modified and upgraded.

Access control systems often use video intercom systems. Substations located at primary entrances incorporate a video camera that records visitors at the door. Depending on the vendor-supplied features, video cameras may take close-up as well as wide-screen views and cameras may feature pan/tilt/zoom capabilities to provide additional visual data on the visitor. The master station has a video monitor that displays the images produced at the substations. For more information on video camera capabilities and features, refer to Section 8.3.

5.2.2.2 *How the Technology Is Used*

School intercoms allow routine communications between the administration and the school staff and serve as valuable tools during emergencies. They provide voice communication between two or more locations and allow school security staff to monitor audio in substation-equipped areas while the staff

¹⁴ http://www.intercomsonline.com/MURS_Radio...Multi-Use_Radio_Service_Technology_Guide_a/340.htm

remains at the base station. Many access control systems also use an intercom system to screen outsiders before allowing entry into the schools.

5.2.2.3 What Makes the Technology Good?

5.2.2.3.1 How the Technology Works

In an emergency, students and teachers can alert the front office staff and request help by pressing a single button on the intercom. PA systems can be activated through an intercom system to notify the entire school of the emergency. These systems can send unique emergency tones or prerecorded messages (e.g., “lockdown” and “take cover”) so actions can be taken immediately.

Intercoms associated with an access control system allow school staff to initiate the screening process before allowing a visitor access. Once the visitor provides identification (ID) and a reason for visiting via the video-enabled intercom, school staff controlling the door can perform the verification process and unlock the door remotely if requirements are satisfied.

5.2.2.3.2 Differentiators

Hardwired intercom systems that operate only over handsets can be more limiting in terms of operability and maintenance. Hands-free communications as a default with an option for private conversations over a handset offers a combination that will suit most environments. Noisy spaces, such as gyms or auditoriums, may be better served by handset communications as a default. Duplex systems are more convenient and intuitive. Newer IP-based systems offer more flexibility of services and easier maintenance.¹⁵ Wireless systems may be appropriate for schools without sufficient IP infrastructure because the installation costs of wired systems can be daunting. Audio quality and ease of use varies with the system and the installation method, but should be among the primary considerations for intercom systems.

Two-way communications with an option for both public and private conversations differentiate intercoms from personal communications technologies such as radio and phone. Intercoms also tend to be easier to use, with one-touch operation and without the need to know appropriate channels or phone numbers.

5.2.2.3.3 Specifications and Features

The area to be covered, geography of the school buildings, regular maintenance, and other factors drive acquisition decisions. Four components are necessary for initial installation: a base station, substations, repeaters (for wireless installs), and speakers. The number of units needed varies by the school’s size, geography, and particular requirements. A single base station may be sufficient for a small school. However, multiple base stations may be needed if intercom calls can be received at multiple locations. For instance, during regular hours, calls can be received by a base station at the main office and after-hour calls may be received at a base station in a control center located elsewhere.

In addition, the adaptability of the base station is an important feature. The base station should accommodate additional substations and multiple configurations of substations to account for different operating environments. The base station should be upgradable but not require upgrade when substations are modified or added. Systems that allow more than one base station can offer more flexibility

¹⁵ http://www.clearcom.com/upload/download/Clear-Com_HybridNetwork_WhitePaper.pdf

but require careful system configuration and supporting procedures. The number of components (such as substations and speakers), features supported by them and locations to install will affect the cost. From a cost perspective, wireless units may be more attractive because installation costs can be lower if the signal is guaranteed to be clear and reliable at all locations.

Hardwired systems should be configured appropriately by the installer. Both wireless and IP-based systems can experience interference or competition for a communications path, so specifications of the underlying wireless or IP system must be sufficient to support the intercom system. Information technologists should be involved in any decision about intercom systems because they will be responsible for maintaining the system and the underlying communication pathways, whether wired, wireless, or IP-based. Power supply must also be considered, and the base station and substations should include battery backup.

5.2.2.3.4 *Effectiveness*

It is hard to assess the effectiveness of intercoms and PA systems for security purposes. The technology is most commonly used for routine school communications not related to school safety. This daily use likely helps ensure regular maintenance and confirms the quality of transmission, both important factors for effective communications in a school safety event. Intercom systems integrated with access control technologies are highly dependent on the cameras, access control system, and procedures associated with access control; therefore, independent metrics of effectiveness are not available. The authors found no data on the effectiveness of this technology relative to school safety.

5.2.2.3.5 *Policy Impacts*

An intercom may be one of several notification systems, including phones and video feeds, so the school's policy on the use of intercoms should be documented. Schools should document policies for selecting the type of intercom matching the everyday requirements as well as the type of threat, the school environment, and the budget. Districts must decide between wired and wireless systems, video and non-video systems, IP and non-IP systems, and simplex and duplex systems for both new construction and retrofitting of existing schools. Uniform acquisition policies may make systems easier to maintain across the district, but officials need to account for the differing needs of new and existing construction. They should also have standard policies in place for calculating the number of base or master stations, substations, and speakers needed based on building layout, floor plans, and budget.

5.2.2.4 *Concerns About the Technology*

5.2.2.4.1 *General Discussion (What It Does Not Do)*

Intercoms, by design, cater to centralized communications, with the base station controlling the information provided to each substation. Although the setup makes communication with the base station much more efficient, it does not allow for communication between substations. In this way, the technology cannot replace point-to-point technologies such as two-way radios or phones.

Intercoms integrated with access control systems provide front office personnel a way to interact with visitors without giving them access, but they are only one part of the access control solution. Poor processes or malfunctioning systems may result in threatening individuals gaining entry into schools.

5.2.2.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

Because of the reliance on the base station, if administrators or first responders do not have access to the base station, their ability to use the intercom system is limited. Many systems include a means to access the base station remotely, but this may only allow users to send a message or otherwise limit the full functionality of the base station.

Substations associated with access control systems are susceptible to vandalism or tampering if they are not in a secured location. If these access control intercoms include video, the camera must provide a clear wide-angle background view to be sure all potential visitors are visible and can be identified before access is granted.

5.2.2.4.3 *Possibilities for Misuse*

Prank calls can be made from substations. Some vendors provide a direct-dial remote means to access the base station, so this capability should come with a password and procedures should be established to prevent misuse.

5.2.2.4.4 *Liability and Safety Concerns*

The individuals who have access to the base station are responsible for communications over the intercom. Policies and procedures should be established to ensure proper use of the system to limit liability concerns.

5.2.2.4.5 *Privacy Concerns*

Systems without a handset on the substations should not be used to communicate any information that might be considered confidential or be legally restricted.

If the intercom system incorporates video, there may be legal or policy guidelines for storing and protecting any images of students or visitors.

5.2.2.4.6 *Accommodations Needed for Disabilities*

School security staff should make the devices and units accessible to the physically challenged. For the hearing impaired, an alternate means of communication must be implemented because intercoms rely on audio.

5.2.2.4.7 *Policy Concerns*

School officials and first responders should determine how intercoms are used in an emergency and include these in the overall school safety plan. Because intercoms are predominately used for day-to-day operations, much of the policy associated with these systems will not address use during acts of criminal violence. This policy will likely be contained in the school safety plan, but should be replicated in the general policy for using intercoms to ensure awareness among users.

For intercoms associated with access control systems, policies and procedures should accommodate the system as configured to ensure proper access is granted.

5.2.2.5 Cost Considerations

The costs of intercoms can vary based on a number of factors. Some cost factors to consider are described in Table 5-4.

Table 5-4 Intercom Cost Considerations

Cost Factor	Cost Description
Acquisition	At least one base or master station (intercom plus other features) is necessary. Depending on the setup, schools may want more than one base station. Each room on the intercom also needs a substation with microphone and speaker. Wired systems will require wiring purchase, but even wireless will require power connections. Wireless systems may require repeaters. IP-based systems should operate using existing IP infrastructure in school, but Information Technology (IT) personnel should be consulted before purchase.
Installation	Depends on design, but wiring for wired systems and power access for all systems.
Operation and labor	For the regular staff, intercom monitoring or intercom communications should be part of their routine duties. If intercom stations have to be monitored during non-school hours, personnel cost needs to be factored.
User training	Minimal for using the technology. Policies and procedures regarding intercom use may require training.
Maintenance	Minimal, but should be part of regular maintenance routine.
Consumables	Backup batteries
Energy and energy dependency	Systems should have battery backup.
Software licenses	Depends on vendor
System integration	Depends on vendor

5.2.2.6 Emerging Technologies and Future Considerations

IP-based wireless intercom systems may become more prevalent in the future because these systems can support a wide range of evolving features and are easy to use, install, and maintain.¹⁶ IP-based systems depend on the school IT infrastructure for support.

5.2.2.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 5-5 presents examples of known vendors of intercom and PA systems; however, it is not comprehensive and other vendors may exist. The list is current as of 13 October 2015.

¹⁶ <https://kintronics.com/network-attached-amplifiers-ip-intercoms-work-2/>

Table 5-5 Intercom and PA System Vendors

Vendor	Website
Aiphone	www.aiphone.com
Cyclop Security Co. Ltd.	http://cyclopsecurity.manufacturer.globalsources.com
Jade Electronics Co. Ltd	http://jade-elec.manufacturer.globalsources.com
Panasonic	www.panasonic.com
Shenzhen Tongwei Video Electronics Co. Ltd	www.tongweisz.com
Two Way Direct, Inc.	www.TwoWayDirect.com
Valcom	www.valcom.com
Visiplex	www.visiplex.com
Zenitel	http://www.zenitel.com

5.2.2.8 Further Reading

Additional resources to consider are:

- Gottfredson, G. D. (2001) "What schools do to prevent problem behavior and promote safe environments." *Journal of Educational and Psychological Consultation*, 12(4), 313–344.
- Tursman, C. (1989) "Safeguarding schools against gang warfare." *Safetylit*, 46(5): 8-9, 13–15.

5.2.3 EMERGENCY CALL BOXES

5.2.3.1 Introduction

Emergency call boxes are devices that connect a person in distress with first responders at the push of a button. They are used to provide timely assistance and mitigate the consequences of a crime in progress. Commonly, these are deployed in environments where personnel access is common both during and after business hours but 24/7 monitoring is not feasible. Emergency call boxes act as force multipliers in isolated areas and are usually deployed in buildings, parking lots, parking decks, and open spaces. They are more commonly used on college campuses where people are more likely to travel between buildings, particularly during evening hours, but are also valuable for K-12 schools used for community functions when classes are not in session.

Emergency call boxes are usually identified by easily recognizable signs and blue lights. They have a call button that automatically connects the caller to the campus security office, a remote monitoring station, or a police radio network. This allows responders to speak with a potential victim and to document an event as it unfolds.

Emergency call boxes can be broadly categorized in two groups: wall-mounted and tower (short or tall) (Figure 5-3). Wall-mount units and shorter towers are appropriate indoors where ceiling height is limited, whereas tall towers can be 8 to 10 feet tall for greater visibility outdoors. Many call boxes use bright colors (such as yellow or red), are labeled with words such as "POLICE" or "EMERGENCY," and include a flashing strobe. Some units include two buttons—one for reaching the security staff or police and another for reaching a parking attendant (for non-emergency conditions like a dead car battery).



Figure 5-3 Examples of Emergency Call Boxes

5.2.3.2 How the Technology Is Used

When a person presses the call button on the emergency call box, the unit immediately activates the emergency strobe light so others in the vicinity are notified and can offer help. This strobe light will remain flashing until a remote attendant turns it off, eliminating the possibility that an attacker can disable the strobe to minimize attention. The emergency call box automatically dials a primary telephone number, or a backup number if the primary number is unreachable (e.g., busy or no answer). A call progress indication—a flashing light, for example—may also be provided for the benefit of the hearing impaired. Once security officers or police answer the call, two-way communication is established and a response can be initiated. School districts usually contract with a local police department or private security firm to provide response to call boxes. This provider must be outfitted with technology to accommodate the system, such as caller id and video feeds.

Many systems provide the location of the call box to the responders; they may also include a video camera that can be triggered to record when the call button is pressed. Further enhancements, such as networked cameras near the call box cued to record the event, may provide improved situational awareness for responders.

5.2.3.3 What Makes the Technology Good

5.2.3.3.1 How the Technology Works

Emergency call boxes provide a quick and easy way for the victim of a crime to contact emergency personnel.

5.2.3.3.2 *Differentiators*

One of the primary benefits of emergency call boxes is the ability to directly connect to responders. All systems with built in location capabilities ensure that a responder knows the location of the emergency even if the caller is unable to specify the location. Systems that include video cameras can provide responders additional information and assist in investigation, but are more expensive and require a robust communications capability to transmit video data and possibly additional personnel to monitor the feed. The number of call boxes installed influences the cost, which is proportional to the spacing of the call boxes and the area to be covered. Vendors should provide options on coverage so school officials can easily consider the tradeoff between higher cost and lower coverage. If the system is going to take advantage of an existing communications technology, either wired or wireless, the availability and capacity of this network must be confirmed. Calls from emergency call boxes are low frequency but high priority, and some technologies, such as third-party leased, IP-based communications using older routers, may not be able to accommodate this type of service or may require changes in IP settings that are outside of the control of the school district.¹⁷

5.2.3.3.3 *Specifications and Features*

Emergency call boxes should operate with the press of a single button. Most come with a hands-free speakerphone, but some may include a handset. The emergency call system should communicate the location of the call box when it is used so that responders can dispatch accurately. Boxes installed outdoors should have adequate protection from the elements and be built to withstand expected local weather extremes. Systems that include video cameras have different levels of quality for the video feed and different means to transmit and record this video. Chapter 8 provides more details about video surveillance specifications.

The response assurance depends on several aspects of the system design. One of the most significant decisions for school districts considering this technology is the means of communication between call boxes and the monitoring location. Wireless, cellular, and private branch exchange (PBX) telephone networks in which users share a number of outside lines for making external phone calls, as well as combinations, are all options. School officials must balance the reliability of the communications with the installation costs for the different options. Wireless installation is less expensive, assuming access to electric supply is trivial, but may be more costly to operate and less reliable. Wired installation is highly reliable and may require less maintenance, but installation costs can be prohibitive. To provide comprehensive coverage, site surveys should be conducted to determine the ideal placement of call boxes and antennas. The geography of the area along with the building structures will determine the number of repeaters needed.

No matter what technology is used, call boxes are preconfigured only to send calls to the monitoring station or designated backup locations, which may be on or off campus. Call boxes are preprogrammed to call a specific number; if no connection is established within a preset time, alternative numbers will be called according to a predefined prioritized list. School districts must negotiate ongoing service contracts with responders, and these contracts will determine this prioritized list. Districts must also negotiate software licenses for managing call boxes and for ongoing maintenance contracts for the upkeep of the boxes.

¹⁷ <https://www.safaribooksonline.com/library/view/voip-hacks/0596101333/ch01s07.html>

5.2.3.3.4 *Effectiveness*

The authors found no data on the effectiveness of the technology. Anecdotally, college emergency managers refer to the number of times emergency call boxes are used and the response time, suggesting possible valid metrics for school districts.¹⁸

5.2.3.3.5 *Policy Impacts*

School districts should consider carefully the relevant threats to make sure there are enough attendants to receive the expected call volume from emergency call boxes. Districts must establish regular test plans to ensure call boxes function appropriately and response times are acceptable. Vendors sell polling software that simulates calls originating from call boxes to test whether the units are working per specification. If the system includes video cameras, any policies on storing and securing the video must be accommodated by the system.

5.2.3.4 *Concerns About the Technology*

5.2.3.4.1 *General Discussion (What It Does Not Do)*

The technology is limited to calling a pre-identified number with no option to contact an alternate responder; it also does not guarantee a timely response. A news team interviewing students at San Diego City College learned that the students were frustrated with the response times, which could be as long as 15 minutes, and some did not know how to operate the call boxes.¹⁹ Even though the use of call boxes is uniform and straightforward, training (e.g., at installation and periodically when new students and staff arrive on campus) about emergency call boxes can be beneficial to staff and students in aiding the understanding of what they are for and how to use them. By their nature, call boxes are usually highly visible and in an open area. However, except in high crime areas, acts of criminal violence in schools more often occur indoors and in less public settings, limiting the impact of call boxes.²⁰

5.2.3.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

Power failure or network infrastructure problems can make all boxes non-operational, and the call boxes themselves can be vandalized. Spacing and coverage of an area can affect a potential victim's ability to reach the call box before being attacked.

5.2.3.4.3 *Possibilities for Misuse*

Students may use the emergency call button for non-emergency needs or false alarms.

5.2.3.4.4 *Liability and Safety Concerns*

If a student is attacked after making a call from a call box, the school district may be liable if an investigation determines the response time was too slow.

5.2.3.4.5 *Privacy Concerns*

Schools may need to protect the anonymity of a victim, and the data collected (including video) could contain sensitive information.

¹⁸ <http://www.emergencymgmt.com/safety/College-Campuses-Deploy-Blue-Light-Phones-Opinion.html>

¹⁹ Emergency call boxes: Does the system work? <https://www.youtube.com/watch?v=zYA4-nC9g7k>

²⁰ <http://fairfieldmirror.com/news/emergencycallboxeshelpreduceoncampuscrime/>

5.2.3.4.6 Accommodations Needed for Disabilities

The placement of the emergency button on the units should be within the reach of all individuals.

5.2.3.4.7 Policy Concerns

Policies concerning the quality of service, such as the attendant response time and the type of emergency responders, should be documented, reviewed, and periodically updated. Diligence should be exercised in sharing any sensitive data with others.

5.2.3.5 Cost Considerations

The costs of emergency call boxes can vary based on a number of factors. Some cost factors to consider are described in Table 5-6.

Table 5-6 Emergency Call Box Cost Considerations

Cost Factor	Cost Description
Acquisition	Wall mount units are less expensive than towers, and cameras typically add to the cost. The type of connection for communications and power will dictate need for additional cabling.
Installation	Depends on area covered and communications technology, as well as availability of existing infrastructure. Wired systems will be more expensive, assuming power connections are available.
Operation and labor	Monitoring and response should be negotiated with the vendor or a third party providing the service.
User training	Minimal.
Maintenance	Assume typical telephone line charges.
Consumables	Batteries, if backup desired.
Energy and energy dependency	Electricity; battery backup or generators.
Software licenses	Notification software must be purchased, and many have an annual license fee.
System integration	Integration with existing infrastructure can save installation costs, but will carry its own cost. Video may need to be stored for a certain time and integrated with other video surveillance technology.

5.2.3.6 Emerging Technologies and Future Considerations

Emergency call boxes are likely to be connected to the Voice-over Internet Protocol (VoIP) network in the future. This network is likely to support new features that emerge. Call box management software for collecting and integrating voice and video across other surveillance technologies may be available, especially as surveillance software improves.²¹

The ubiquity of cellphones is making many users reconsider the use of emergency call boxes, even though connectivity through call boxes is much more reliable. While maintenance cost is often a driver of these decisions, it should not be the primary reason to discontinue use. A thorough analysis of usage

²¹ <http://www.campusafety magazine.com/article/Today-s-Emergency-Help-Station-The-Evolution-of-the-Traditional-Call-Box>

statistics should be completed before a district decides to remove emergency call boxes to ensure there will be no significant effect on the school community.²²

5.2.3.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 5-8 presents examples of known vendors of emergency call box systems; however, it is not comprehensive and other vendors may exist. The list is current as of 13 October 2015.

Table 5-7 Emergency Call Box Vendors

Vendor	Website
BearCom	bearcom.com/products/other-solutions/remote-call-boxes/
Codeblue	http://codeblue.com/
Rath Security Emergency	http://www.rathsecurity.com/

5.2.3.8 Further Reading

Additional resources to consider are:

- Dameron, S. L. (2009) “An assessment of campus security and police information on college/university websites.” *Security Journal*, 22(4), 251–268
- Wireless Campus Escort System. <https://www.google.com/patents/US7149533>

5.2.4 TELEPHONE SYSTEMS

5.2.4.1 Introduction

Telephones (landline and cellular) are one of several two-way communications technologies used for school safety. Seventy-nine percent of public schools have telephones, usually landlines, in the classrooms²³; however, available statistics do not address whether these telephones provide convenience, safety, or both. Phone use does not vary by instructional level but varies somewhat by school size—only 73% of schools with less than 300 students have phones in classrooms, whereas 85% of schools with more than 1000 students do have them, and suburban schools are slightly more likely to use phones in classrooms.

5.2.4.1.1 Cellphones in K-12

Cellphones can be valuable backup tools during emergencies in those school districts that maintain cellphones on campus for administrators, crisis team members, and other appropriate adults. However, the use of cellphones by students during school hours has been a hotly debated issue. Cellphones were commonly banned from students during school hours for a variety of reasons ranging from being disruptive to the school environment to cheating and abusing the privilege. With the public’s heightened

²² <https://www.insidehighered.com/news/2010/09/02/phones>

²³ Source of all statistics: Table 1 in Reference 353

awareness of school violence since Columbine, policies regarding student use of cellphones during school hours are changing, although even districts that allow cellphones place restrictions on their use.²⁴

5.2.4.2 How the Technology is Used

5.2.4.2.1 Landline Telephones

Landline telephones remain a viable and widely available means of communication in classrooms, administrative offices, and other locations, making it easy for school staff to alert school officials if a threat is detected. Depending on the policy and protocol established, school staff can contact first responders as well. Emergency contact numbers can be posted near the handsets or be preprogrammed as quick-dial numbers.

Calls originating from phones are routed through the vendor's underlying network via landlines or a cellular network. Larger schools may access landlines through a PBX system. Hosting a PBX in schools reduces overhead telephony costs and can save money for larger schools. This requires a switchboard or some other routing technology. Some new schools or modernized older schools with an IP infrastructure can use VoIP service. A VoIP phone system converts outgoing audio into a digital stream that is transmitted over the Internet, and it converts incoming digital phone signals from the Internet to standard telephone audio. The advantages of VoIP include ease of installation, configuration, and maintenance, lower costs, and access to a wider range of features.

Written directions, placed near each landline phone, can describe the process for making a call during emergencies. In some systems, users can directly dial 911, whereas others require a fourth digit to reach an outside line. Dialing 0 may put users in contact with their school's main office, a district operator or directory, or nothing, depending on the system setup, so policy must be established for any relevant shortcuts. Some systems automatically forward missed calls to a prioritized list of alternate contacts known as a hunt group until someone is reached, so the members of such a group and their call priority on the list must be established; more generally, alternate numbers should be provided for after-hours operations.

5.2.4.2.2 Cellphones

Cellphones are commonplace technology that provides all of the capabilities of landlines along with text, web browsing, and smartphone apps. Schools may choose to replace landlines with cellphones or decline to install landlines in new construction and use only cellphones. However, because cellular signals can be overwhelmed by demand, this option carries with it a significant risk especially during an emergency.

Using group text functions in cellphones offers the capability to reach many people instantaneously, e.g., to warn students of an imminent threat. Texts can also be used to provide parents, teachers, and students with accurate information to help quell rumors and to discourage parents from coming to a school during an event so that responders are not impeded.²⁵ Students can also use their cellphones to convey information during emergencies. After the Chardon (Ohio) High School shooting, students used their phones to call 911 and to let their parents know they were safe. "The school is now considering an update to their plan called ALICE—which stands for alert, lockdown, inform, counter, and evacuate—in

²⁴ Ohio school shooting: Drills, cellphone use paid off (Poll: Should students be allowed to have phones in school?), http://www.cleveland.com/chardon-shooting/index.ssf/2012/02/northeast_ohio_school_district.html

²⁵ <http://mashable.com/2012/12/15/cellphones-school-emergency/>

which cellphones play an important role. For instance, a mass text could direct students in case of a crisis.”²⁶

Smartphones offer further functionality through a wide range of apps that can be installed. Many school safety apps are available on cellphones. For example, a cellphone caller with the MyForce²⁷ app which mimics the function of an emergency call box allowing the caller to immediately get a security agent’s attention just by pressing the logo on the cellphone. When the alert is sent, the agent can determine the location of the caller, track his/her whereabouts, and contact campus security or the police immediately and share the information.

5.2.4.3 What Makes the Technology Good

5.2.4.3.1 How the Technology Works

In the event of an emergency or threatening event, appropriate local authorities are frequently contacted via telephone. School staff use the telephone to notify a student’s parents in the event of a medical emergency or serious injury; they could also be contacted via telephone in the event of a school-wide emergency.

5.2.4.3.2 Differentiators

Telephones are ubiquitous and robust technologies that provide more versatility than radios and other self-contained networks. The technology also has the most active development climate, which means new features are quickly developed and integrated into existing equipment.

Landline phones tend to be more reliable than cellphones and less susceptible to dropped calls and dead batteries. Landlines also convey their physical address immediately to 911 operators; additionally, some alarm companies require landline connections. Landlines may also be preferable over cellphones and radios because they have no distance or coverage area limitations. Landlines, like all phone systems, allow point-to-point private conversations that may not be available over intercom systems. Landlines that connect via VoIP technology may offer additional features and be less expensive to maintain and upgrade.²⁸

The added capabilities of smartphones, especially mobile Internet access and the availability of safety-related apps, increase the breadth and depth of information that can be conveyed to a large group during an event. Cellphones also have a potentially larger user base for private communications, especially in middle and high schools where many teachers and students carry cellphones. This also enables more individuals to provide information to responders, school officials, and parents during an event.

5.2.4.3.3 Specifications and Features

For landlines, the most important specifications for a phone system are the locations where phones will be placed and the number of individual lines the school will lease. For small schools, a small number of phones with dedicated landlines may make the most sense. For medium and large schools it is often advantageous to use a PBX system, where there may be many physical phones but a limited number of outside lines available. This reduces cost by allowing the school system to lease fewer lines. However,

²⁶ Op. Cit. Ohio school shooting

²⁷ <http://myforce.com/>

²⁸ <http://www.techrepublic.com/blog/10-things/10-voip-features-that-can-benefit-your-small-business/>

the system must be specified with good estimates of the number of calls individuals may place at any given time because line availability can be an issue in an underspecified system. This may be even more relevant in an emergency situation when numerous users may be trying to communicate at the same time. VoIP systems use the Internet to make calls, so the number of lines is less relevant but the underlying IP infrastructure must be robust enough to handle the expected call volume. Individual phones can also be equipped with specific upgrades to accommodate the special needs of users. Among these are large buttons, hands-free operation, extra loud ring tones, lights as well as ring tones to indicate a call, and even automated Braille readers.

For cellphones, one of the most important decisions a school district must make is the bring-your-own-device (BYOD) policy. Many schools and other institutions, recognizing the widespread use of smartphones, offer apps and other smartphone services but expect users to have their own device and service plan. This can greatly reduce the acquisition cost for schools, but increases the maintenance cost because any services must be provided for all types of smartphones and service plans. The school system also loses significant control over communications by not specifying the communications device, which may limit the number and types of features and apps provided. If the district decides to provide cellphones to some or all users, they must negotiate with cellphone service providers over types of phones, types of service, data plans, and other relevant features.

5.2.4.3.4 *Effectiveness*

NCES publishes various statistics on the percentage of telephones in classrooms, but has no data on effectiveness. There are no statistics on the percentage of reduction of violence or attacks as a result of telephones in classrooms.

Certain types of phone systems have relevant broad metrics. For VoIP-based landlines, the bandwidth and data speed are relevant; for cellphones, the coverage area, number of dropped calls, and data speed may all be useful for measuring the effectiveness of a phone system in day-to-day as well as emergency operations.

5.2.4.3.5 *Policy Impacts*

Policies established by the school security team should provide guidelines as to when and how the telephone system should be used, and if and how its use should be integrated with other communication systems, such as PA system, intercom, and two-way radios. PBX systems may have the ability to prioritize certain communications, but policies must be established to keep cellular bandwidth open for school officials and first responders.

Cellphones and VoIP phones can have added features for use in either day-to-day or emergency operations. Policy on how these features are used and trained must be established so that they can be used during an event.

5.2.4.4 *Concerns About the Technology*

5.2.4.4.1 *General Discussion (What It Does Not Do)*

Standard telephone service offers few features specific to school safety needs. When an emergency call is placed, there is no prioritization and there is no guaranteed response time from first responders.

5.2.4.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

Calls may be unanswered or lines may be in use by the intended recipient; therefore, features such as call forwarding busy, call forwarding no answer, and hunting for lines may be useful. Cellular connections may experience disruption, and transmissions may be overwhelmed by volume, especially in an emergency.

During emergencies, the public telephone network can experience congestion due to increased call volumes and/or damage to network facilities. The Government Emergency Telecommunications Service (GETS)²⁹ and the Wireless Priority Service (WPS)³⁰ provide national security and emergency preparedness personnel priority access and prioritized processing in the local and long-distance segments of the landline networks and the cellular network, greatly increasing the probability of call completion during an emergency.

Phone lines may be cut intentionally or by utility work, natural disasters, or explosions. Cellphones may be lost, damaged or inaccessible during an emergency.

5.2.4.4.3 *Possibilities for Misuse*

A ringing phone in the classroom can be disruptive, but many schools prevent this by answering all calls in the main office and forwarding the calls to individual classrooms only if they need immediate attention.

5.2.4.4.4 *Liability and Safety Concerns*

School districts must provide the ability for people with disabilities to communicate with emergency services. If the district is using a BYOD policy, there must be a means to communicate with users who do not have a smartphone or cannot use the services provided by the district because of the type of cellphone or calling plan they use.

5.2.4.4.5 *Privacy Concerns*

None identified by the authors.

5.2.4.4.6 *Accommodations Needed for Disabilities*

Users may require human-operated services for media and mode (voice, text, and video) translation during phone conversations.

5.2.4.4.7 *Other Issues*

During emergencies, cellular networks may be inundated with calls from students, staff, and parents, thus making it difficult for school administrators to reach first responders.

5.2.4.4.8 *Policy Concerns*

None identified by the authors.

²⁹ <https://www.dhs.gov/about-gets>

³⁰ <https://www.dhs.gov/about-wps>

5.2.4.5 Cost Considerations

Costs are a major concern for many school districts in installing and maintaining telephones and telephone outlets in classrooms. The costs of telephones vary based on a number of factors. Some cost factors to consider are described in Table 5-8. While negotiating with the service provider, schools should make sure the local calling area covers the boundaries of the school district.

Table 5-8 Telephone Systems Cost Considerations

Cost Factor	Cost Description
Acquisition	Costs of individual phones may vary. Most schools will need a switchboard and may require additional wiring installed in the school. If cellphones are used, a repeater may need to be installed in the school building.
Installation	Installation of lines may be necessary for landline systems.
Operation and labor	If a switchboard is used, someone in the school office must be assigned to answer calls.
User training	VoIP phones and some features may require some training.
Maintenance	Routine cleaning and inspection
Consumables	None
Energy and energy dependency	Minimal
Software licenses	If VoIP or cellphones are used, some programming of features and apps and associated software, may be necessary.
System integration	N/A

5.2.4.6 Emerging Technologies and Future Trends

VoIP phones are becoming more common and will continue to replace traditional phones. Newer technology and enhanced data plans are allowing for VoIP connections over cellphones, which can increase the availability of security and other features.³¹

5.2.4.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 5-9 presents examples of known vendors of telephone systems; however, it is not comprehensive and other vendors may exist. The list is current as of 13 October 2015.

Table 5-9 Telephone Systems Vendors

Vendor	Website
AT&T	www.att.com
Comcast	www.xfinity.com
Sprint	www.sprint.com
Verizon	www.verizon.com

³¹ [https://www.visiongain.com/Report/1327/Voice-over-Internet-Protocol-\(VoIP\)-Market-Forecast-2014-2019](https://www.visiongain.com/Report/1327/Voice-over-Internet-Protocol-(VoIP)-Market-Forecast-2014-2019)

5.2.4.8 Further Reading

Additional resources to consider are:

- Fickes, M. (1999) “The ABC’s of Security Technology.” *Under Siege: Schools as the New Battleground*
- Simone, R. et al. (2012) *Indicators of School Crime and Safety*, NCES 2013-036/NCJ 241446

5.3 ONE-WAY COMMUNICATIONS

5.3.1 EMERGENCY NOTIFICATION SYSTEMS

5.3.1.1 Introduction

An ENS disseminates emergency messages from a single source, usually a school official or emergency responder, to multiple recipients. ENSs may use one or more methods to communicate, but usually require recipients to request inclusion on a list and to provide addressing information for the notification. Some of the most common platforms include phone calls, text messages, email, smartphone alerts, PA system announcements, rich site summary feeds, social media (e.g., Twitter, Facebook), and physical or electronic message boards.

ENSs allow officials to deliver time-sensitive consistent messages to a broad population of self-identified recipients. This personalization increases the speed and accuracy of notification by simultaneously reaching all members of the target audience for the message. In an emergency, ENSs can provide information and instructions to threatened individuals to help them change their behavior or actions and avoid a threat.

5.3.1.2 How the Technology Is Used

Modern ENSs often require minimal installation. Many vendors operate an Internet service that officials can log into from any web-enabled device. ENS administrators, commonly school officials or members of law enforcement, are the people responsible for managing the system and disseminating the emergency notifications and should have an assigned authority over an emergency. ENS recipients self-identify as interested parties who want to receive emergency notifications. ENSs used in the elementary schools are more often designed with the assumption that school staff and parents will be the recipients, whereas ENSs used in middle and high school include the student population as recipients because many of these students carry cellphones and smartphones.

The emergency notifications instruct recipients to perform or not perform a specific action.³² Emergency notifications can be used for a variety of situations, ranging from active shooters and imminent threats to general weather warnings and road closures.

5.3.1.3 What Makes the Technology Good?

5.3.1.3.1 How the Technology Works

ENSs used by schools allow for quick, consistent dissemination of relevant information during an emergency. Some systems integrate across multiple communication methods, including phone, text, email,

³² Interview with Paul Dillion (University of Maryland Baltimore County) on 11 September 2015.

and social media. An effective school ENS allows administrators to generate a single message and rapidly send it to recipients on a variety of platforms at once.³³

Predefined templates built for specific scenarios can help school officials quickly draft an emergency notification. ENS administrators only need to collect the information expected and populate the template. This helps administrators understand what information must be collected and speeds up the creation of the message.

One of the simplest and most effective ways to optimize performance of an ENS is through initial and reoccurring training to teach appropriate reactions to specific situations. Other good practices include limiting the number of emergency notifications transmitted, creating targeted audiences using ENS group templates, and using specific graphics and colors in the emergency alerts (e.g., red indicates danger, blue indicates safe).

5.3.1.3.2 Differentiators

ENSs are more specifically targeted and enable faster dissemination of information than traditional approaches such as radio or TV announcements or phone trees, and they allow administrators to control the content of the message. In contrast to mass text messages or emails, integrated systems also increase the likelihood of communicating information by delivering over more than one platform. Multiple platforms also help overcome potential access issues for users with special needs.

5.3.1.3.3 Specifications and Features

Because many ENS solutions are web-based, there is little need for special hardware. ENSs will have a variety of platforms for message delivery, and while each district may have different reasons for using certain platforms, the ENSs that give users the most flexibility are generally preferred. Most systems essentially allow an unlimited number of recipients, but systems with a limit on the number should be carefully evaluated to ensure they meet the needs of the school district.

5.3.1.3.4 Effectiveness

ENSs should be tested regularly to ensure messages get delivered to all intended recipients. This testing should include a means for users to indicate their receipt of the message and a mechanism to update the recipient list. Tests should occur across all platforms and be well publicized.³⁴ In general, ENSs work better when they are publicized, and response rates in tests may be more indicative of awareness of the system than its functionality. Low response rates in tests are common, not because users do not receive a message, but because they are unaware of the system and the testing.³⁵

5.3.1.3.5 Policy Impacts

Policy should specify the types of emergencies that the ENS will be used for and the scope and nature of messages for each type. School officials should designate ENS administrators and their relationship to the school district and first responders to ensure accurate, coordinated information is sent. Policy should cover the types of recipients expected and how the recipient list will be maintained and updated.

³³ <http://www.campussuite.com/top-school-emergency-notification-systems-review/> (accessed 22 January 2016)

³⁴ http://www.mhec.org/sites/mhec.org/files/20150312emergency_notification.pdf (accessed 2/1/16)

³⁵ <http://pro.sagepub.com/content/53/18/1466.refs>

Policy must be developed on the training necessary for administrators. A policy on publicizing the ENS and testing it with the user base is also necessary.³⁶

The FCC and FEMA have implemented Wireless Emergency Alerts (WEAs), which provide alerts (e.g., presidential alerts, threats to safety or life alerts, or Amber alerts) to specific locations or recipients with certain smartphones.³⁷ School districts should partner with their local emergency management agency to access WEAs automatically for distribution over their ENS.

5.3.1.4 Concerns About the Technology

5.3.1.4.1 General Discussion (What It Does Not Do)

ENSs are intended solely for one-way communications. This limits the ability of the recipients to convey information that is relevant to the incident back to the official sending the message. Section 5.2 on two-way communications describes technology solutions for this type of interaction.

5.3.1.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Recipients will ignore the alerts if the system is overused and too many are sent out.³⁸

5.3.1.4.3 Possibilities for Misuse

Only appropriate administrators should be given access to the system. Communication with the provider is required. Because an ENS constitutes a one-way communication, it is difficult to ensure all recipients receive the message.

5.3.1.4.4 Liability and Safety Concerns

Sending incomplete or inaccurate information can lead to confusion and unsafe actions or decisions by recipients.

5.3.1.4.5 Privacy Concerns

Although there are no real privacy concerns for users, administrators must ensure contact information is protected, the correct information is disseminated, and no sensitive information is released.

5.3.1.4.6 Accommodations Needed for Disabilities

A well-designed ENS generally transmits messages across multiple platforms, which makes this a particularly useful technology for reaching individuals with disabilities who can elect the method by which they prefer to receive messages.

5.3.1.4.7 Policy Concerns

Schools will probably want to document who is allowed to generate ENS messages and under what circumstances.

³⁶ <https://police.colorado.edu/sites/default/files/Emergency%20Response%20and%20Evacuation%20Policy.pdf>

³⁷ <https://www.fcc.gov/guides/wireless-emergency-alerts-wea>

³⁸ <http://www.preparis.com/blog/5-reasons-why-mass-notification-systems-are-difficult-to-use-for-emergency-notification/>

5.3.1.5 Cost Considerations

The costs of ENSs can vary based on a number of factors. Some cost factors to consider are described in Table 5-10.

Table 5-10 Emergency Notification System Cost Considerations

Cost Factor	Cost Description
Acquisition	Many vendors provide the ENS using a web-based interface or software-as-a-service (SaaS). In these cases, there is no requirement to acquire a system and the school district pays a monthly fee to use the services provided by the vendor.
Installation	None
Operation and labor	ENS administrators will have to spend some time configuring the system and setting up templates.
User training	Administrators must learn how to create an alert in the proper format and ensure familiarity.
Maintenance	Because many ENS vendors take on the responsibility of maintaining the system, school districts must establish a maintenance contract with the vendor. Some contracts charge a monthly maintenance fee, whereas others specify a per-incident fee. System upgrades should also be negotiated.
Consumables	None
Energy and energy dependency	None
Software licenses	Negotiated along with purchase and maintenance contracts.
System integration	May depend on the number of platforms that the ENS communicates over, but depends on the sophistication of the system.

5.3.1.6 Emerging Technologies and Future Considerations

Systems that can easily add the ability to communicate through new platforms, such as new social media apps, are easier to adapt to changing technologies.

5.3.1.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 5-11 presents examples of known vendors of ENSs³⁹; however, it is not comprehensive and other vendors may exist. The list is current as of 1 February 2016.

³⁹ <http://www.campussuite.com/top-school-emergency-notification-systems-review/>

Table 5-11 Emergency Notification System Vendors

Vendor	Website
e2Campus	http://www.e2campus.com/
Blackboard Connect 5	https://www.blackboardconnect.com/signin/default.aspx
Rapid Responder	http://www.preparedresponse.com/Rapid-Responder-Campus-Safety.html
School Messenger	http://www.schoolmessenger.com/school-emergency-alerts/
One Call Now	http://www.onecallnow.com/who-we-serve/education/
K12 Alerts	http://www.k12alerts.com/webcorp/homepage.html

5.3.2 BULLHORNS

5.3.2.1 Introduction

A bullhorn is a portable, handheld, cone-shaped device used for directional amplification of voice or other sounds (e.g., a whistle). The words bullhorn and megaphone are used interchangeably. The sound of a voice is amplified and may result in distortion, but it can be heard over a long distance. In general, these devices are lightweight, weatherproof, and battery operated; their effective range varies as a function of battery power.

In 2006, the U.S. DoED's Emergency Response and Crisis Management Technical Assistance Group released Volume 1, Issue 2, of their *Helpful Hints* series.⁴⁰ This document, along with many others, recommends an emergency kit be prepared and available for certain school staff, such as administrators and nurses. Although the contents of these kits vary from one school to another, a bullhorn is one of the recommended items to include.

5.3.2.2 How the Technology Is Used

Bullhorns are a mature and commonplace technology, and are often used in situations unrelated to safety to provide instructions or information to large crowds in open spaces. In emergency situations, they are used for crowd and traffic control or for broadcasting evacuation and event control instructions.

5.3.2.3 What Makes the Technology Good?

5.3.2.3.1 How the Technology Works

A bullhorn is a simple, inexpensive tool typically used to amplify verbal instructions. Bullhorns enable on-the-spot broadcast messages or previously recorded messages or other sounds, such as a siren or whistle.

5.3.2.3.2 Differentiators

A bullhorn is one of several technology options for broadcasting a message. Other options include a PA system or a two-way radio, but the bullhorn is inexpensive technology, highly portable and operates on an independent power supply.

⁴⁰ http://rems.ed.gov/views/documents/HH_GoKits.pdf

5.3.2.3.3 *Specifications and Features*

Bullhorns are handheld devices, usually made of acrylonitrile butadiene styrene (ABS) plastic and weighing between 2 and 6 pounds. The distance they can transmit sound is a function of the power of the device, and most range from 4 to 35 watts. This provides a projection distance of 500 feet to a half mile, depending on the setting. Most have volume controls and special sounds, such as a siren, that can be broadcast. Some even include the ability to record short messages that can be repeated periodically.

5.3.2.3.4 *Effectiveness*

The authors found no data on the effectiveness of bullhorns at reducing acts of criminal violence.

5.3.2.3.5 *Policy Impacts*

The school's policy on when to use bullhorns should be documented.

5.3.2.4 *Concerns About the Technology*

5.3.2.4.1 *General Discussion (What It Does Not Do)*

Bullhorns have limited range, usually measured in hundreds of yards. Even within a certain distance, the number of recipients can be limited to as few as 50 because of acoustic effects in crowds. Because message recipients are generally located within visual distance, feedback on the effectiveness of the message being transmitted is generally rapid.

5.3.2.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

Taking the bullhorn to prevent its use was the only method of circumvention identified by the authors.

5.3.2.4.3 *Possibilities of Misuse*

Bullhorns should be secured to prevent someone using it for unauthorized purposes.

5.3.2.4.4 *Liability and Safety Concerns*

None identified by the authors.

5.3.2.4.5 *Privacy Concerns*

None identified by the authors.

5.3.2.4.6 *Accommodations Needed for Disabilities*

Staff and students with hearing loss will not be able to hear messages. Staff with speech impairments can use prerecorded messages.

5.3.2.4.7 *Policy Concerns*

The school crisis management team or the security staff should have written guidelines on who should use a bullhorn under what conditions and how to use the device. When developing effective messages, it is helpful to develop them in advance of an emergency.

5.3.2.5 Cost Considerations

The costs of bullhorns can vary based on a number of factors. Some cost factors to consider are described in Table 5-12.

Table 5-12 Bullhorn Cost Considerations

Cost Factor	Cost Description
Acquisition	Higher priced models support three modes (talk, siren, and whistle) and have greater range.
Installation	None
Operation and labor	None
User training	None
Maintenance	Minimal battery charging and possible cleaning or storage.
Consumables	Batteries
Energy and energy dependency	None
Software licenses	None
System integration	None

5.3.2.6 Emerging Technologies and Future Considerations

None identified by the authors.

5.3.2.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 5-13 presents examples of known vendors of bullhorns; however, it is not comprehensive and other vendors may exist. The list is current as of 13 October 2015.

Table 5-13 Bullhorn Vendors

Vendor	Website
Anchor Audio PA Equipment	www.schooloutfitters.com
AmpliVox Portable Sound Systems	https://www.schoolsin.com/
Caliphone Products	www.schooloutfitters.com
Champion Bull Horns	http://www.megaphones.org/megaphones
Dick's Sporting Goods	http://www.dickssportinggoods.com/
Hamilton Electronics	http://www.projectorscreenstore.com/shop-by-brand-hamilton-electronics-pa-systems-bullhorns-and-megaphones.html
Quake Kare	http://www.quakekare.com/bullhorn
Rhode Island Novelty	http://guide.alibaba.com/shop/rhode-island-novelty-8-supporters-megaphone-with-siren-sound-colors
Schools In	https://www.schoolsin.com/AMP-Mity-Meg-Megaphones.html
Thunderpower	www.Thunderpowermegaphones.com

5.3.2.8 Further Reading

An additional resource to consider is:

- Patterson, P. E. et al., “Audiovisual Equipment Standards,” <http://eric.ed.gov/?id=ED002706>.

5.3.3 DIGITAL SIGNS AND BILLBOARDS

5.3.3.1 Introduction

Digital signs and billboards are a form of technology that displays video, text, or other multi-media content. They are usually placed in public areas for informational or advertising purposes. If a computer is deployed with them, or they are connected to an application on the Internet, their display can quickly be changed or updated; this makes them particularly useful in communicating information about an emergency.

5.3.3.2 How the Technology Is Used

Schools commonly use digital signs for day-to-day communication of general information. They are usually LED or flat screen displays placed in prominent locations indoors or outdoors, such as main entrances and cafeterias. Some are text only, but many, especially indoor digital signs, can display graphics and video.

These signs can also be used in the event of an emergency to communicate with staff and students. Their prominence and availability make them an obvious means of communication during an event or during safety training drills.

Examples of indoor and outdoor digital signage boards are shown in Figure 5-4.



Figure 5-4 Indoor (left) and Outdoor (right) Digital Signage Boards

5.3.3.3 What Makes the Technology Good

5.3.3.3.1 How the Technology Works

In its most basic implementation, a digital sign consists of a playback device (such as a computer, video cassette recorder, or digital video disk player) connected to a display. Depending on the application, the display might be a small liquid crystal display (LCD) screen, a plasma display panel, or even a video wall composed of a number of connected screens. In recent years, several factors have combined to make

digital signage a more powerful, eye-catching, and affordable display medium. Key factors include the availability of high-speed Internet access, large format displays like plasma screens and LCD panels, and compression formats that can compress large amounts of content into small file sizes.

The controller, typically a personal computer or other media playback appliance, controls the content of the display. The playback device uses a digital storage medium (such as a hard drive or solid-state flash disk) to store digital content locally, ensuring smooth playback. In many cases, the device can be remotely managed over the Internet to allow for content updates, schedule changes, and compliance reporting.⁴¹

5.3.3.3.2 *Differentiators*

Digital signs can be integrated with other mass communication technologies to provide greater probability of reaching a larger audience. During routine use, digital signs display non-emergency messages, but during emergencies, the display can be overridden with an emergency alert message.

Some vendors are flexible in their offering from a la carte specific components (e.g., software only) to a full turn-key solution, where a third party offers a product or service that is designed, supplied, built, or installed fully complete and ready to operate by the end user (e.g., hardware, software, and professional services).

5.3.3.3.3 *Specifications and Features*

Digital signs range in capability from displays that can only display text to those that can display high-definition full-color graphics. Although some LED displays can display low-resolution graphics on outdoor signs, LCD or plasma screens are preferable for displaying graphics on indoor digital signs.

Each display also requires a player. Some systems allow multiple signs to be controlled from the same player, which can reduce acquisition costs. These devices are generally connected to their digital signs with high-definition multimedia interface (HDMI) cables, but other options may be available with some players. Many players automatically display common formats such as PowerPoint and .gif files, whereas others require proprietary software.

There are two models for delivering content to the digital sign—push deployment and pull deployment. In the push model, content for the sign is pushed to the IP addresses of the players connected to the screens; in the pull model, the player connects to a vendor-provided web service and pulls the content.

A district can store and manage its digital sign content with a SaaS solution or a server-based solution. In a SaaS solution, all of the district's digital sign content is hosted by the vendor's data centers and published with an Internet connection; server-based solutions require the purchase of server software and hardware.

5.3.3.3.4 *Effectiveness*

The authors found no data specific to the effectiveness of digital signs during safety events.

⁴¹ https://www.wirespring.com/pdf/intro_to_digital_signage.pdf, retrieved 2/9/16.

5.3.3.3.5 *Policy Impacts*

A school's policy on how to use digital signs during an emergency should be documented and address their use in conjunction with other communication systems. This also affects the choice of system administrators because school officials should normally have primary control over the message, but they may need to delegate that control to first responders in crisis situations.

School districts must also determine any changes to the safety plan or training regarding the use of digital signs in an emergency. This may include special graphics or colors that staff and students should look for in case of an event to help direct their actions. This extends to policy on how digital signs may be used to communicate that a threatening situation has ended as well as any special graphics or colors that may accompany that message.

5.3.3.4 *Concerns About the Technology*

5.3.3.4.1 *General Discussion (What It Does Not Do)*

This technology is useful for communicating basic instructions in the event of a significant emergency, but is not useful for preventing or mitigating acts of criminal violence. In the event of a significant emergency, the technology is only effective if its use during an emergency has been well communicated to students and staff and if they are accustomed to getting information from the digital signs during normal operations, and they have access to the signs during an event, thus such signs have very limited use during a lockdown situation.

5.3.3.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

This technology relies on power and Internet connections, so if either is unavailable the digital signs cannot be effectively used in an emergency. In addition, digital signs and monitors can be vandalized.

5.3.3.4.3 *Possibilities for Misuse*

Standard system security controls should apply to the digital sign system as with all controlled access systems in the school district.

5.3.3.4.4 *Liability and Safety Concerns*

None identified by the authors.

5.3.3.4.5 *Privacy Concerns*

None identified by the authors.

5.3.3.4.6 *Accommodations Needed for Disabilities*

Digital signs are not appropriate for visually impaired persons. Alternate arrangements must be made to reach these recipients.

5.3.3.4.7 *Policy Concerns*

None identified by the authors.

5.3.3.5 Cost Considerations

The costs of digital signs can vary based on a number of factors. Some cost factors to consider are described in Table 5-14.

Table 5-14 Digital Sign Cost Considerations

Cost Factor	Cost Description
Acquisition	Software is usually licensed. In general, software supporting interactive features is more expensive. Industrial-grade monitor prices depend on type of monitor and features (e.g., touch screen capability).
Installation	Not available
Operation and labor	Minimal (can be part of routine tasks)
User training	Minimal initial training
Maintenance	Minimal
Consumables	None
Energy and energy dependency	Ordinary power requirements (120 volts) for charging the battery
Software licenses	Software licenses must be renewed periodically
System integration	N/A

5.3.3.6 Emerging Technologies and Future Considerations

Digital signs are likely to get cheaper as the LCD monitor market continues to mature. Users may not have to buy extra media players or small computers to drive the content on digital signs. One vendor (Samsung) introduced a system-on-chip that eliminates the need for a separate media player and cuts energy costs. User friendliness will be enhanced and content creation and user interface will be simplified.

5.3.3.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 5-15 presents examples of known vendors of digital signage products; however, it is not comprehensive and other vendors may exist. The list is current as of 13 October 2015.

Table 5-15 Digital Sign Vendors

Vendor	Website
AD vantage LED Signs	www.advantageledsigns.com
Fourwinds Interactive	www.fourwindsinteractive.com
Rise Vision	www.risevision.com
Scala	www.scala.com
The Marlin Company	www.themarlincompany.com
UCview, Inc.	www.ucview.com
Visix	www.visix.com
Watchfire Signs	www.watchfiresigns.com

5.3.3.8 Further Reading

An additional resource to consider is:

- Yackey, B. (2011) *A Beginner's Guide to Digital Signage*. NetWorld Alliance, LLC.

5.3.4 DATACASTING

5.3.4.1 Introduction

Datacasting refers to a technology that can transmit encrypted data files, such as blueprints, student databases, and surveillance video, over existing digital television (DTV) signals instead of using Internet or cellular systems.

There are three distinct aspects to the datacasting system: information collection and processing, transmission processing, and reception processing (Reference 336).

5.3.4.2 How the Technology Is Used

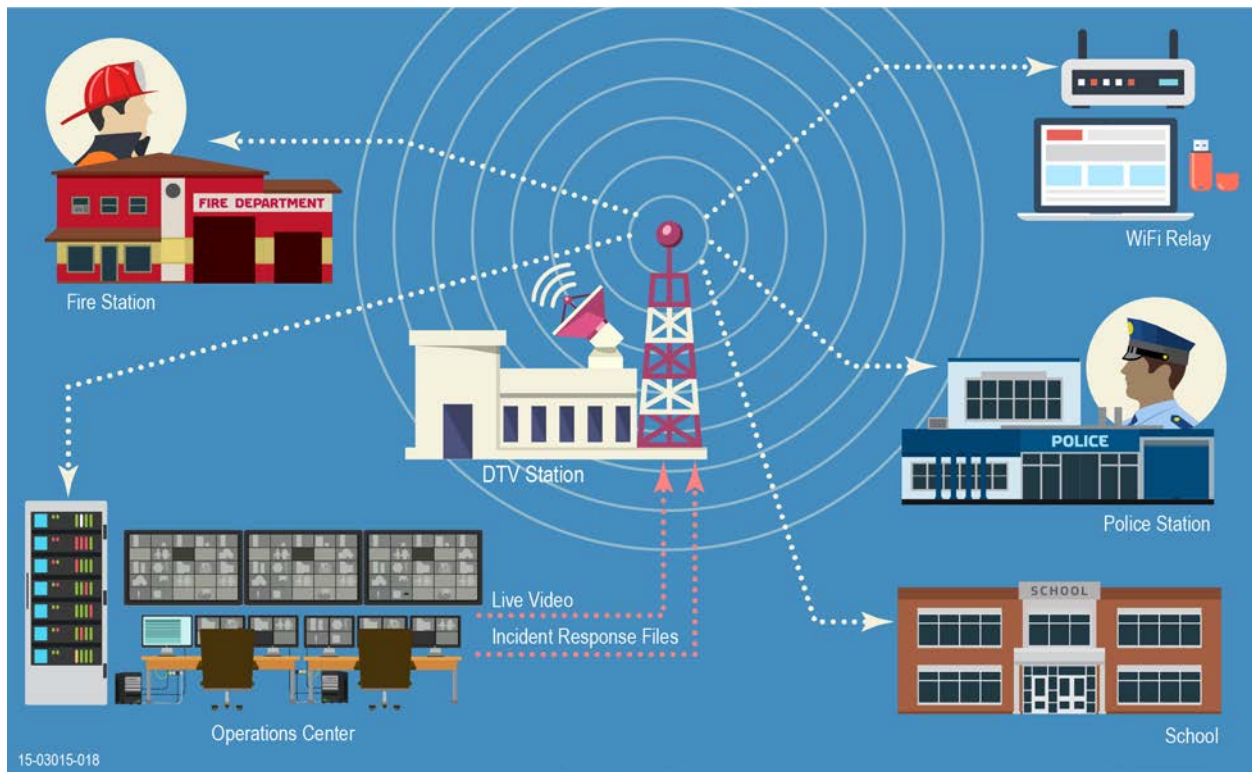
Although datacasting has been implemented by school districts in Kentucky, Wisconsin, and Tennessee to complement distance-learning programs, at the time of publication the Clark County School District (CCSD) in Nevada is the only school district known to have implemented datacasting specifically for school safety. In the event of a school emergency, police dispatchers within the Emergency Operations Center can activate the datacasting system and transmit information such as building plans, evacuation plans, and student records including photos, medical conditions, and disciplinary reports to incident managers who have a receiver. This may be most useful for time-sensitive information such as video feeds from the school, and the bandwidth provided by datacasting can facilitate this type of information sharing. Additionally, information can be pulled from their integrated Milestone Video Management System (Reference 336)

5.3.4.3 What Makes the Technology Good?

5.3.4.3.1 How the Technology Works

DTV broadcast signals do not use all of the available transmission bandwidth. Datacasting is the process of inserting IP data into the DTV transmission along with the standard TV programming. Any digital information that can be created on a computer can be inserted and transmitted within the TV broadcast signal (Reference 86).

The required data are transmitted over TV signals and captured by a receiver that translates the signal into information that can be accessed on a computer (Figure 5-5). Datacasting is a one-way communication channel because the signal must be transmitted by a TV station. Sending the data to the TV station for broadcast requires another communications channel such as Internet or cellular (Reference 368).



Source: SpectraRep

Figure 5-5 Diagram of Data Transmitted to Receivers via Datacasting

The Warning, Alert, and Response Network (WARN) Act of 2006 requires Public Broadcasting Service (PBS) stations, as a condition of FCC licensing, to carry emergency messaging datacasts provided by FEMA to PBS and distributed to stations using the PBS distribution infrastructure (Reference 86).

5.3.4.3.2 Differentiators

The WARN Act included resources for stations to harden their transmission systems and to acquire the equipment to reliably carry, receive, and integrate emergency messaging datacasts into the station's local broadcast channel. This system has been installed and is operational in all PBS member stations across the country (Reference 86).

Unlike cellular networks, PBS station broadcasts do not suffer from failure caused by high call volume experienced during natural emergencies such as Hurricane Katrina, or manmade incidents such as the Boston Marathon bombing, and therefore are still able to broadcast emergency information. Cellular towers are also susceptible to power outages and damage from severe weather, whereas PBS stations have continuity of operations plans in place to ensure their ability to broadcast during large-scale emergencies (Reference 336). Because the TV system is significantly more robust than Internet and cellular systems, datacasting can hold a distinct advantage over other wireless communications.

5.3.4.3.3 Specifications and Features

Datacasting is primarily a software system that allows digital data to be transmitted over existing TV broadcast signals, and then reconverted into computer readable data through a small antenna and

translation software at the receiving end (Reference 87). The vendor specifies the hardware and software needed to integrate with equipment at the TV station.

A datacasting system requires the cooperation of the local TV station. PBS stations traditionally performed a critical role in public safety by broadcasting information for the Emergency Broadcast System (EBS). Although the national notification system has evolved, PBS stations continue to provide a source of emergency information when telephone and cellular systems have shut down, and therefore may be considered reliable partners for datacasting.

5.3.4.3.4 *Effectiveness*

PBS is an organization that provides a national infrastructure for interconnection of public TV stations across the country. PBS member stations collectively provide the largest coverage of the U.S. population of any single entity, with a high resilience against weather and manmade disruption because of the robustness of its hardware and the overlapping coverage in many locations. Approximately 98% of the U.S. population resides in areas capable of receiving DTV transmissions (Reference 86). With increasing demands on cellular networks, availability of bandwidth to transmit large video and audio files is often limited, particularly during a local emergency. Using the excess transmission capacity of local TV stations provides a reliable, secure transmission system and frees up cellular resources for other needs.

With only the CCSO school district using datacasting for school safety, there is limited data regarding its value. The CCSO system has been activated during football games between rival high schools, which have traditionally been associated with an increase in violent crime. However, no metrics were collected to indicate any effect the additional source of data had upon criminal activity. The effectiveness of transmitting data over TV signals was demonstrated during a summer forest fire when first responder command posts were set up in the empty CCSO schools. The local TV station transmitted weather data from the National Weather Service to classroom televisions using the EBS (Reference 336).

5.3.4.3.5 *Policy Impacts*

Because datacasting depends on the availability of relevant data, a critical concern is ensuring the system can access data needed during an emergency. Memoranda of Understanding (MOUs) should be established as soon as possible to specify types of data that will be shared between agencies.

5.3.4.4 *Concerns About the Technology*

5.3.4.4.1 *General Discussion (What It Does Not Do)*

Datacasting provides an alternative to Internet- and cellular-based data systems. However, because information must be coded as TV data and broadcast over TV wavelengths, it is a one-way system. There is no integrated way to receive feedback from users to determine that the messages have been received. Also, it is not currently feasible to have mobile TV broadcast stations.

5.3.4.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

During an emergency, schools need the ability to send critical information to the TV station for broadcast. This requires a secure, high-speed Internet connection between the school and the TV station. This requirement may present a limitation for rural schools, or during times when Internet connections are unavailable or overburdened by other transmissions.

A datacasting system relies on the availability of updated, relevant information. In the event of a school incident, it is critical that information provided to law enforcement be accurate. Data must be maintained by the school district and updated as frequently as it changes.

5.3.4.4.3 Possibilities for Misuse

Once data files are authorized for sharing, unauthorized access to the data should be prevented during transmission. Data files can be encrypted before being transmitted to the TV station and remain encrypted through the datacasting process until decrypted by the receiving software. Datacasting should be considered at least as secure as the Internet, possibly more so because only a small number of incidents have been reported where an unauthorized message was transmitted over a TV signal (References 71 and 382); of those incidents, there are no reports of an encrypted TV signal being intercepted by an unauthorized receiver.

5.3.4.4.4 Liability and Safety Concerns

None identified by the authors.

5.3.4.4.5 Privacy Concerns

A critical concern is protecting the privacy of student and staff records, as well as any emergency procedures or evacuation plans that could be misused. The school district should own most of the data, including video camera feeds, medical and disciplinary records, building plans, and incident management plans.

There are particular concerns with disclosing personal information about juveniles. The CCSD datacasting system has the capability to remove data from the system once an incident is closed. Although protected data feeds are no longer available, policies are required to ensure that recipients delete any files saved to an individual computer (Reference 336).

5.3.4.4.6 Accommodations Needed for Disabilities

The message generation and data receipt processes are conducted on a computer. To be compliant with the ADA, the hardware and software used to create, transmit, and receive the information must be usable by people with disabilities.

5.3.4.4.7 Policy Concerns

Sharing data with local law enforcement requires careful consideration of privacy issues and the establishment of new school policies and MOUs between schools and external agencies to define how and when to share data.

5.3.4.5 Cost Considerations

The costs of datacasting can vary based on a number of factors. Some cost factors to consider are described in Table 5-16.

Table 5-16 Datacasting Cost Considerations

Cost Factor	Cost Description
Acquisition	The complete system can be expensive and may not include the cost of additional receivers and adapters.
Installation	Included
Operation and labor	Minimal: Datacasting system implementation would allow emergency dispatchers to access information contained within school databases and deploy it to first responders. Some effort might be needed to ensure data are formatted for transmission.
User training	Less than 1 day per user, with periodic refreshers if the system is not used frequently.
Maintenance	Included under contract with vendor.
Consumables	None
Energy and energy dependency	No additional costs.
Software licenses	Expensive annual software license fee.
System integration	Varies; some will be included in the initial setup; additional integration must be contracted separately.

5.3.4.6 Emerging Technologies and Future Considerations

As of the writing of this report, TV broadcast receivers must remain stationary to function properly because the modulation standard for home reception was based on the use of a rooftop antenna. New receivers have been developed to receive mobile broadcasts and are now available in certain cellphone and tablet models, as well as add-on adapters (commonly called dongles) and universal serial bus (USB) adapters for laptops. The ability to receive datacast signals in a moving vehicle may drive interest in use by first responders and subsequently generate additional interest in developing and using the technology in schools (Reference 86).

Users can respond from the field and request additional information using cellular Internet or radio messages, but integrating a reliable return path into the datacasting system for two-way communications is likely to increase acceptance of the technology. With increasing dependence on smartphones, the ability to receive datacasts on a cellphone would make datacasting even more versatile (Reference 58).

5.3.4.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 5-17 presents examples of known vendors of datacasting products; however, it is not comprehensive and other vendors may exist. The list is current as of 15 October 2015.

Table 5-17 Datacasting Vendors

Vendor	Website
SpectraRep	http://www.spectrarep.com

5.4 CONCLUSION

Communication is one of the most vital capabilities for school officials and first responders in the event of an act of criminal violence or natural disaster. Many of the technologies discussed in this chapter pertain to mass communication, especially the one-way communication technologies. These are usually relevant during and after major emergencies that relate to school safety. However, they may also be an effective means of communicating school safety plans during normal operations. Although not the focus of this study, awareness of and training on school safety plans is a primary driver of school safety initiatives, and these plans should include concepts for incorporating all available communications methods for disseminating appropriate information.

Two-way communications technologies often allow for one-to-one and private conversations, and therefore may be useful during major events as well as small-scale acts of criminal violence in schools. In this role, communications primarily play a role in the response and recovery phases of an event, but may have some impact during the event to mitigate harm. As society has moved to mobile communications with the ubiquity of cellphones, schools should plan for and adapt to this technological shift. Hardwired, location-dependent communications are still more robust and have a place in schools, but the increased reliability of mobile platforms along with their much greater versatility make these technologies more appealing in the future.

Per Article 9(b) of the Convention on the Rights of Persons with Disabilities,⁴² people with disabilities must have access to information, communications, and other services, including electronic services and emergency services. Both auditory and visual (including written) means of communication have been reviewed in this chapter, but school officials should ensure that the combination of technologies used can accommodate all potential users.

Nearly all communications technologies in this chapter can be considered dual use, and are primarily designed for day-to-day, non-emergency operations. This should be considered a benefit from a cost perspective and an operational standpoint. Naturally, costs are lowered if a technology has multiple uses beyond an emergency situation, but it is important to consider the technology's use in such a case when making a purchase decision. The added benefit of dual-use technology is the increased attention to training and maintenance. Systems purchased strictly for response to crime may see little to no use in many schools and thus fall into disrepair without any indication, even if reasonable maintenance is performed. Dual-use technology used on a daily basis does not face this risk, and thus more likely to be available in the event of an emergency.

In conclusion, school districts should be sure to include safety considerations when making any purchase of communications technology. Any new technology should be incorporated in the school safety plan and in training exercises. Schools should coordinate with first responders when making communications technology decisions to ensure the systems can interoperate or integrate as needed. Lastly, school districts should recognize the full benefit of communications technologies by considering relevant school safety scenarios.

⁴² United Nations Human Rights, Article 9 – Accessibility. Retrieved from <http://www.ohchr.org/EN/HRBodies/CRPD/Pages/ConventionRightsPersonsWithDisabilities.aspx#9>

Chapter 6. TECHNOLOGY REVIEW – LIGHTING

Kelly A. O'Brien, PhD

6.1 INTRODUCTION

For this technical review, lighting is discussed as it relates to violent crime prevention and detection in schools. For the most part, lighting in this context is referred to as security lighting. This is different from task lighting (e.g., the lights that enable work performance in a classroom, office, laboratory, etc.), safety lighting (e.g., streetlights adjacent to a sidewalk that prevent trips and falls at night), and illuminated signs. Security lighting can be installed either inside or outside the school building. Because the types of bulbs used and the applications are somewhat different, these two types of lighting are described separately.

It is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district prior to purchasing a safety or security technology. Table 6-1 presents the means by which the study team evaluated lighting capabilities, aligned with the Federal Emergency Management Agency (FEMA) mission areas: Prevention, Protection, Mitigation, Response and Recovery.¹ This assessment combines the opinion of security subject matter experts and the informed judgment of the authors who evaluated the technologies. Reviewing this table provides a summary of the areas of school security and safety for which lighting may be best suited.

¹ The preparedness cycle consists of the following five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.
- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

In general, appropriately installed lighting can help prevent crime and protect persons and property from criminal acts. Proper lighting can also serve as a response mechanism if it is used with a motion sensor. When lighting is used to illuminate the scene for a video camera, it can be used to recover from and investigate violent crime by having usable video footage.

Table 6-1 Lighting – Technology Impact Summary

Lighting	Prevention	Protection	Mitigation	Response	Recovery
Indoor lighting	LOW Lights can give the appearance of activity, which may cause a would-be intruder to avoid the area	MEDIUM Passersby can see inside and notify the authorities of the presence of an intruder	NONE No effect on mitigation noted	CAUTION Law enforcement response may require control of lighting	MEDIUM Cameras may require adequate lighting to capture actionable images
Outdoor lighting	MEDIUM May deter a would-be intruder	MEDIUM Passersby can see that an intruder is present and notify the authorities	NONE No effect on mitigation noted	CAUTION Law enforcement response may require control of lighting	MEDIUM Cameras may require adequate lighting to capture actionable images
<p>Impacts as they relate to a technology's ability to impact a school's ability to <i>prevent, protect, mitigate, respond, or recover</i> from an incident.</p> <p>High: Technology is expected to have a <i>significant</i> impact.</p> <p>Medium: Technology is expected to have <i>some</i> impact.</p> <p>Low: Technology is expected to have <i>little</i> impact.</p> <p>None: Technology is expected to have <i>no</i> impact.</p> <p>Caution: Technology will have an impact; however, it may also have unintended consequences.</p>					

Subsections 6.3 and 6.4 discuss indoor and outdoor security lighting, respectively, in terms of the range of uses, what makes the technology good, concerns about lighting, future trends, costs, and current vendors.

6.2 UTILIZATION STATISTICS

While the research team did not find statistics on the usage of security lighting for schools, most state and local building codes require security lighting (Reference 97). Many states have adopted the *International Building Code* (Reference 165), mandating the need for lighting outside of buildings. The Illuminating Engineering Society of North America's (IESNA's) *Guideline for Security Lighting for People, Property, and Public Spaces (G-1-03)* (Reference 164) is another reference that is adopted extensively by state and local building code authorities. It can be assumed that almost all schools will have indoor and outdoor security lighting.

6.3 INDOOR SECURITY LIGHTING

Indoor lighting can help prevent, protect, and aid in recovery from school violence and, to a lesser extent, can help in the response, especially at night. Specific scenarios and technology specifications are discussed next.

6.3.1 INTRODUCTION

Indoor security lighting can illuminate an indoor setting either continuously or intermittently through use of a switch, timer, or motion-activated sensor.

The following terms are relevant to indoor lighting:

- Illumination terms
 - **Lumen:** The quantity or flow of light emitted by a lamp.
 - **Illuminance:** The concentration of light over a surface [measured in lux or foot-candles (fc)].
 - **Lux:** The unit of illuminance, measuring luminous flux per unit area. It is equal to one lumen per square meter. One lux equals 0.0929 fc.
 - **Foot-Candle:** Measure of brightness when the light reaches 1 foot from the source.
 - **Watt:** A measure of electrical energy used.
 - **Brightness:** Intensity of the sensation of light as seen by the eye.
 - **Glare:** Excessive brightness.
 - **Luminaire:** The lighting unit or fixture that consists of one or more lamps and the other parts that protect and position the lamp and connect it to a power source.
 - **Ballast:** An auxiliary piece of equipment designed to start and properly control the flow of power to discharge light sources such as fluorescent and high-intensity discharge (HID) lamps.

Indoor bulb types are displayed in Table 6-2.

Table 6-2 Examples of Indoor Light Bulbs






Bulb Types	Description	Examples
Compact fluorescent lamp (CFL)	Designed to replace incandescent bulbs in existing and new installations. They use fluorescent technology that has been adapted to fit into existing incandescent fixtures.	
Fluorescent	Produces white light when an electrical current passes through a phosphor-coated tube containing low-pressure mercury vapor.	

Table 6-2 Examples of Indoor Light Bulbs (Continued)

Bulb Types	Description	Examples
Halogen	Generates a bright light by passing an electrical current through a tungsten wire surrounded by halogen gases such as iodine or bromine.	
Incandescent	Generates light by passing an electrical current through a tungsten wire.	
Light-emitting diode (LED)	Solid-state device that emits light when electrons move in a semiconductor material. This is a rapidly growing light source option.	

6.3.2 HOW THE TECHNOLOGY IS USED

Indoor security lighting provides light inside a school building. It may be used to deter criminals by making it appear that people are still present or by providing a pool of light so that passersby and neighbors can see and report questionable activity after schools are no longer in session, frequently after dark.

In general, indoor security lighting is the same lighting used during normal school operational hours, but it is used to prevent crime when a building is unoccupied because the building appears to be occupied. It is often used at a lower capacity than normal occupied use; that is, fewer lights remain on or an occupancy or motion sensor activates them. Occupancy sensors can be used in conjunction with indoor lighting to detect when a person has entered the room. This allows the lights to be turned on when movement is detected, and then turned off automatically when motion has not been detected for a set period of time.

If closed-circuit television (CCTV) is being used on a school campus, the image captured may be unusable if the proper lighting is not in place. Lighting quality as well as flicker rate may not be compatible with CCTV systems, so this should be considered. Fluorescent lighting flickers at a 60-Hz rate that interferes with the CCTV 30-Hz rate; fluorescents also contain MV that interferes with the color fidelity of video (Reference 317). Although LED lights flicker, it is at a rate that is usually imperceptible to the human eye and simple modifications, like rectification, make the effect even less.

The state of Virginia has published a school safety inspection checklist for its public schools that addresses best practices for indoor lighting (Reference 371):

Interior lighting is another area that should be included in the scheduled maintenance plan. The plan should list the school's procedures for reporting light outages also.

The Virginia interior lighting safety inspection checklist includes the following items (Reference 371):

- Do all rooms, stairwells, and halls have proper lighting?
- Are these areas included in the school's scheduled maintenance plan?
- Does the plan address procedures for reporting light outages?

6.3.3 WHAT MAKES THE TECHNOLOGY GOOD?

6.3.3.1 How the Technology Works

The types of indoor lighting are discussed here in terms of performance.

- **Fluorescents and CFLs:** These bulbs create twice the light and half the heat of an incandescent bulb of the same wattage. CFLs use 80% less power than a standard incandescent. Although they have a longer life span than incandescent bulbs, they can cost substantially more. However, the operating costs are much lower because they consume much less power and last approximately eight times longer. They contain small amounts of mercury, which is an environmental hazard, and therefore have special disposal requirements. Compared to incandescent lights or LEDs, fluorescent bulbs may need a warm-up time to reach full brightness (Reference 282).
- **Halogen:** These lamps are approximately 25% more efficient than incandescent lamps. The typical lifespan is twice as long as an incandescent bulb at 2,000 hours (Reference 287). Halogen lamps use 70% less power than a standard incandescent bulb. Halogens generate a lot of heat and any commercial applications of halogen lamps should comply with Underwriters Laboratory Standard No. UL-153 (Reference 349).
- **Incandescent:** These bulbs are the least efficient and most expensive to operate, with a relatively short life span of about 1,000 hours (Reference 282). They are also being phased out of production, according to a law passed by Congress in 2007 (Reference 365). Although they are not a realistic option for indoor school security lighting, this type of bulb can serve as a baseline due to their familiarity to many readers.
- **LEDs:** LED lamps have been advocated by the U.S. Department of Energy as the newest and best environmental lighting method (Reference 359). LED lamps use only 10% of the power a standard incandescent bulb. The lifetime of LEDs is also much longer—50,000 to 80,000 hours.

Occupancy sensors turn lights on when an individual enters the sensor's field of view. They can control one lamp, one fixture, or many fixtures and can be used for all types of lighting. Two sensor types are discussed in general here; please refer to Chapter 4.3 for a detailed discussion of sensor mechanisms.

- Passive infrared (PIR) sensors react to changes in heat, such as the pattern created by a moving person. The control sensor must have an unobstructed view of the area being scanned. Doors, partitions, stairways, etc., can block motion detection and reduce sensor effectiveness. The best applications for PIR occupancy sensors are in open spaces with a clear view of the area being scanned.
- Ultrasonic sensors transmit sound above the range of human hearing and monitor the time it takes for the sound waves to return. A break in the pattern caused by any motion in the area triggers the control. Ultrasonic sensors are less impacted by obstructions and best for areas with cabinets and shelving, in restrooms, and for open areas requiring 360-degree coverage.

Some occupancy sensors use both PIR and ultrasonic technology, but are usually more expensive.

6.3.3.2 Differentiators

For a school, the decision to use one indoor security lighting technology over another likely would be made on the basis of lifetime cost. In general, indoor task lighting is already necessary; additional security lighting can be provided in a cost-effective way. No system integration is required, although lighting can certainly be integrated with physical security information management (PSIM) systems (Subsection 7.3.2), surveillance cameras (Section 8.3), and/or alarms and occupancy sensors (Section 4.3).

6.3.3.3 Specifications and Features

For indoor security lighting, the technical specifications for the most part are not unique to security because functional lighting will be necessary in a school and security plays a secondary role for the interior lighting. Therefore, the requirements for illumination and cost of running lights during operating hours are likely to be the driving factors when selecting indoor lights.

There are a few specifications that are useful when planning or assessing the lighting levels of a school interior at night when not in use:

- For areas where identification of persons and objects (e.g., packages, trucks) may take place, there should be illumination levels of at least 2 fc (per IESNA) (Reference 282). For reference, an office for daytime use is about 50 fc.
- For CCTV cameras, the minimum level of light is 0.5 fc for detection, 1 fc for recognition, and 2 fc for identification (Reference 4). A detection task involves determining whether an object is present. A recognition task determines the type of an object, such as a person versus a car. An identification task discerns a specific object, such as a woman or a man (Reference 151).

6.3.3.4 Effectiveness

The research team did not find statistics on the effectiveness of indoor lighting on reducing violent crime in schools. Because the majority of violent crimes at schools happen during transition times either during lunch hours or just before or after school, the effect of nighttime indoor security lighting is not readily apparent (Reference 10).

6.3.3.5 Policy Impacts

The use of indoor security lighting may have an impact on energy-conservation policies in the school. For example, if a school district has an existing policy to conserve energy by turning indoor lights off at 6 pm, the security plan may call for security lighting to remain on until sunrise. This would have to be resolved at the district policy level.

6.3.4 CONCERNS ABOUT THE TECHNOLOGY

6.3.4.1 General Discussion (What It Does Not Do)

Lighting can aid in the detection of intruders or provide a deterrent to individuals trying to gain unauthorized access to the school building, but does nothing to prevent or slow physical access.

6.3.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

There are two potential vulnerabilities for indoor security lighting: tampering and loss of power. During an intentional or unintentional power failure, emergency lighting would be available, but security lighting typically would not be (Reference 282). Generators could be used to provide backup power to everyday school systems as well as security systems and lighting.

Another concern is that students or others may tamper with light switches or automated sensors. These devices should be situated in such a way that minimizes tampering opportunities.

Luminaires themselves may be tampered with by students or others who would commit a violent act. This is especially a concern for lighting for CCTVs. The location of lighting for CCTVs should be such that it is not easy to break the lamp, deface it, or render it inoperable. If a person were able to tamper with the CCTV light, the resulting video may not be usable for verification of a crime or for forensics.

6.3.4.3 Possibilities for Misuse

The author did not identify any likely misuses for indoor lighting.

6.3.4.4 Liability and Safety Concerns

Schools should carefully consider where indoor safety lighting is most appropriate and ensure increasing lighting in one area does not displace crime to another less-lighted area.

6.3.4.5 Privacy Concerns

The author did not identify any privacy concerns related to the use of indoor lighting.

6.3.4.6 Accommodations Needed for Disabilities

Switches intended for public use should be accessible to people with disabilities.

6.3.4.7 Other Issues

No additional issues were identified by the author.

6.3.4.8 Policy Concerns

Schools with existing programs to conserve energy may need to modify policies to allow the use of lighting during non-working hours. For example, if a school district has an existing policy to conserve energy by turning indoor lights off at 6 pm, the security plan may call for security lighting to remain on until sunrise. This would have to be resolved at the district policy level.

6.3.5 COST CONSIDERATIONS

As previously discussed, the operating cost of incandescent lamps is the highest. Overall, fluorescent lighting is the least expensive, but LEDs are quickly gaining ground as a realistic option for school lighting. The maintenance costs for LEDs are the lowest, because the lamps last a very long time and therefore do not need to be changed as often. They also use the least power.

The formula to determine the cost to operate a light source is as follows (Reference 282):

$$\text{Watts} \times \text{Hours} = \text{Watts Hours}$$

$$\text{Watts Hours} \div 1000 = \text{Kilowatt Hours}$$

$$\text{Kilowatts Hours} \times \text{Cost of 1 kW per hour} = \text{Cost per Hour}$$

For indoor lighting, little training is required to operate or maintain lighting. Table 6-3 provides cost impacts.

Table 6-3 Indoor Security Lighting Cost Considerations

Cost Factor	Cost Description
Acquisition	Varies; identified products ranged from approximately \$73 to more than \$487 per luminaire.
Installation	Can be significant if security lighting is not considered during construction. Potentially need to install infrastructure electrical wiring as well as fixtures, switches, sensors, and timers. Labor costs associated with the installation.
Operation and labor	Minimal (turn on switch if not automated).
User training	Little training is required to operate or maintain lighting.
Maintenance	Minimal routine cleaning per manufacturer's instructions. Traditional fluorescent tubes need to replace ballasts periodically. Bulbs need to be replaced periodically. There is a wide range of bulb life. This is a cost driver.
Consumables	Lamp bulbs need to be replaced. There is a wide range of bulb life. This is a cost driver.
Energy and energy dependency	Usually alternating current (AC) power; seldom direct current (DC) (battery) power. Energy efficiency is a cost driver.
Software licenses	None
System integration	Can be integrated with motion sensors or set on timers. Can be integrated with backup generator power. Can be integrated with cameras, alarms, and sensors.

6.3.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

For indoor security lighting, the trend is toward the use of LEDs as the light source (Reference 335). These are the most environmentally friendly lamps. LED lamps use only 10% power compared to a standard incandescent bulb. The lifetime of LEDs is also much longer—50,000 to 80,000 hours.

6.3.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 6-4 provides a sample of known vendors of indoor lighting; however, it is not comprehensive and other vendors may exist. The list is current as of 4 September 2015.

Table 6-4 Indoor Lighting Vendors

Vendor	Website	Notes
GE Lighting North America	http://www.gelighting.com/LightingWeb/na/solutions/indoor-lighting/	LED, halogen, HID, fluorescent, CFL, occupancy sensors
Lithonia Lighting	http://www.lithonia.com/pt/commercial+and+industrial+indoor/#.Vemc4KPD-AI	LED, fluorescent, HID
Grainger	http://www.grainger.com/category/ecatalog/N-/Ntt-Indoor+Lighting+Fixtures?cm_sp=CS_Banner-_Lighting_L1_buckets-_Indoor_Lighting	LED, halogen, HID, fluorescent, CFL, occupancy sensors
Seesmart	http://www.seesmartled.com/product/ourproducts/	LED
Williams	https://hewilliams.com/catalog/?brand=downlighting#.VemkX6PD-AI	LED, CFL, HID, incandescent, fluorescent

6.4 OUTDOOR SECURITY LIGHTING

Outdoor lighting can help prevent, protect, and aid in recovery from school violence and, to a lesser extent, help in the response. Specific scenarios and technology specifications are discussed next.

6.4.1 INTRODUCTION

Outdoor security lighting can illuminate an outdoor setting either continuously or intermittently through use of a timer or motion-activated sensor.

The illumination terms introduced in Subsection 6.3.1 are relevant to outdoor security lighting as well.

Outdoor bulb types are displayed in Table 6-5.

Table 6-5 Examples of Outdoor Light Bulbs









Bulb Types	Description	Examples
Electroluminescent	Similar to fluorescent lights, but they do not contain mercury and are more compact.	
Fluorescent	Tubes coated with phosphor containing low-pressure MV that produce white light. They are not often used outdoors (except for signs) because they have a lower light output than other options.	
Halogen	Incandescent bulbs containing halogen gases such as iodine or bromine.	

Table 6-5 Examples of Outdoor Light Bulbs (Continued)

Bulb Types	Description	Examples
High-intensity discharge (HID) Note: This term identifies four types of bulbs that produce light inside gas-filled tubes by means of an electric arc between tungsten electrode	<i>MV</i> : Similar to fluorescent, these also pass electricity through a gas.	
	<i>Metal halide</i> : Used for sports stadiums, because they imitate daylight conditions and colors appear natural. These complement video surveillance systems.	
	<i>High-pressure sodium (HPS)</i> : Often used for streets and parking lots, these are a good solution for seeing more detail at a greater distance in fog.	
	<i>Low-pressure sodium (LPS)</i> : More energy efficient than HPS lamps.	
Incandescent	Most common residential lights, consisting of an electrical current passing through a tungsten wire to produce light.	
Light emitting-diode (LED)	Solid-state devices that emit light by the movement of electrons in a semiconductor material. This is a rapidly growing light source option.	
Quartz	Very bright lights with a rapid onset similar to incandescent. They are frequently used at a high wattage.	

6.4.2 HOW THE TECHNOLOGY IS USED

Outdoor security lighting is used to create a deterrent to intrusion and to enable detection of crimes. Whether lighting is an effective crime control method depends on the adequacy of the lighting. If the lighting is absent and the building is in darkness, an offender will have trouble doing the work necessary to gain access. Offenders would have to bring their own light source, which would enable detection by passersby, but also tie up one hand (e.g., holding a flashlight). This inconvenience may actually prevent crime. However, if the lighting is dim, the offender has just enough light to access the building, while escaping visual detection by passersby and authorities. If the lighting is bright, it can afford an offender enough light to work, but simultaneously enables detection by others, thereby deterring or preventing crime. Another consideration is that intruders can actively exploit glare caused by security lighting, which could allow them to commit crimes without being detected (Reference 67).

Although case law supports outdoor lighting as an indicator of efforts to provide a safe environment, this conventional wisdom is being questioned by security specialists (Reference 29). This is discussed in greater detail in Subsection 6.4.6.

Outdoor lights can be set on timers to turn lights on and off automatically when needed. They can also use photoelectric cells to turn the lights on and off automatically in response to natural light. Street lamps in neighborhoods often use this type of switch.

As with indoor lights, motion-activated PIR sensors can be used in conjunction with outdoor lighting to detect when a person is present on the school property. This allows the lights to be turned on once movement has been detected and then turn off automatically.

If there are exterior video surveillance systems, proper lighting needs to be provided. Metal halide lamps are best for this application, because of their color rendering, but they are expensive to install and maintain (Reference 282).

The state of Virginia has published a school safety inspection checklist for its public schools and it addresses best practices for outdoor lighting (Reference 371):

Lighting should allow the identification of a face from a distance of approximately 30 feet for someone with normal vision. Lights should be inspected regularly to ensure they are in working order.

The Virginia exterior lighting safety inspection checklist includes the following items (Reference 371):

- Are exterior lights adequate?
- Is there lighting at all building entrances?
- Is there lighting at all potential intrusion sites?
- Do athletic facilities have adequate lighting?
- Are all lights mounted 12 to 14 feet high?
- Do exterior lights reduce shadowed areas near the school?
- Do lights have break-resistant glass?
- Are light lenses cleaned annually?

6.4.3 WHAT MAKES THE TECHNOLOGY GOOD?

6.4.3.1 How the Technology Works

The types of outdoor lighting are discussed here in terms of performance (Reference 67). One measure of performance is how accurately colors are rendered by the light source, known as the color rendering index (CRI). This is a scale of 1 to 100; the higher the number, the better the accuracy at depicting color (Reference 97).

- **Incandescent:** These are the least efficient and most expensive to operate, with a relatively short life span. They are not a realistic option for outdoor school security lighting, but it is useful to mention them as a comparison baseline.
- **Fluorescent:** These are energy efficient and have good color quality but cannot be dimmed easily. They are not often used outdoors (except for signs), because they have a lower light output than other options.
- **MV:** These are more energy efficient (use less energy to produce the same amount of light) and have a longer life span similar to fluorescents. They have a high CRI, which allows witnesses of criminal acts to accurately describe colors seen in this light. However, they take several minutes to produce full light output. These lamps exceed 24,000 hours in life span.
- **HPS:** These are energy efficient but have a low CRI (Reference 97). Everything appears to have an orange glow. They are a good solution for seeing more detail at a greater distance in fog. These also take several minutes to produce full light output. They have a lamp life of 24,000 hours.
- **LPS:** These are more energy efficient than HPS but possess limited color rendering. Objects appear to have a yellow color. They have a life span of 18,000 hours.
- **Metal halide:** These are energy efficient and have good color rendering. They are the preferred outdoor lamp for video surveillance systems. It takes several minutes to produce full light output. They have a life span of 3,000 to 20,000 hours, depending on wattage.
- **Quartz:** These are very bright lights with a rapid onset similar to incandescent. They are frequently used at a high wattage, making them excellent for use along perimeters. They have a life span of 2,000 hours.
- **Electroluminescent:** These are similar to fluorescent lights, but they do not contain mercury and are more compact. Their life spans range from 2,000 to 50,000 hours.
- **Halogen:** These increase the efficiency of a plain incandescent lamp by about 25%. They have excellent color rendition. Full light output is available instantly. They have a life span of 2,000 hours.
- **LED:** These have been advocated by the U.S. Department of Energy as the newest and best environmental lighting method (Reference 359). LEDs use only 10% power compared to a standard incandescent bulb. The lifetime of LEDs is also much longer—50,000 to 80,000 hours.

Figure 6-1 shows an example of a parking garage retrofit, which changed from 175-watt HID metal halide lighting to 60-watt C2D LED lighting with a resultant cost savings of 65% without maintenance.

Motion-activated sensor performance is discussed in Section 6.3.

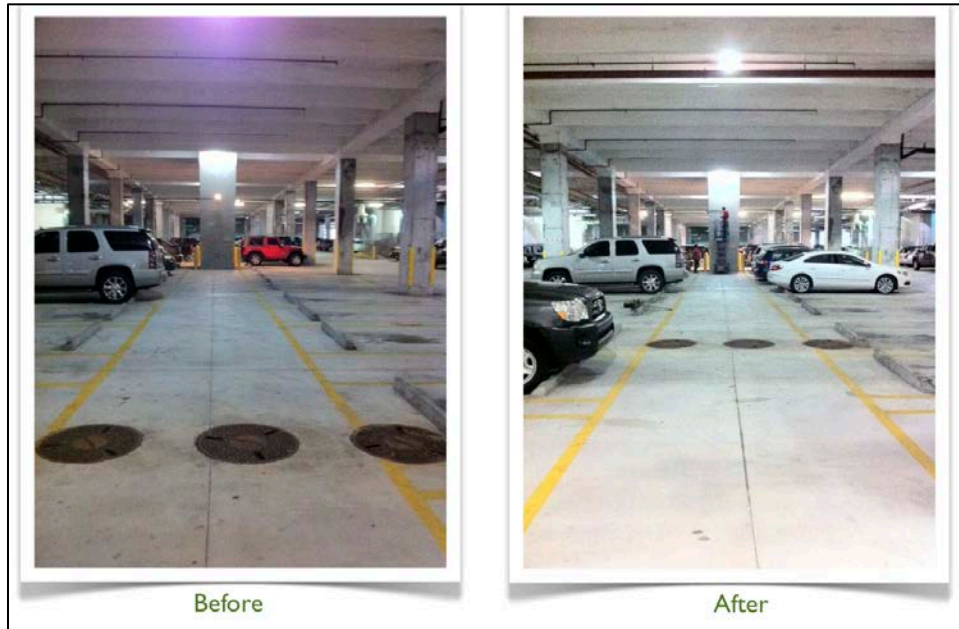


Photo: LED Source®

Figure 6-1 Garage Retrofit

6.4.3.2 Differentiators

For a school, the decision to use one outdoor security lighting technology over another likely would be made on the basis of lifetime cost. In general, outdoor safety lighting to prevent accidents is already necessary; additional security lighting can be provided in a cost-effective way. No system integration is required, although lighting can certainly be integrated with PSIM systems (Subsection 7.3.2), surveillance cameras (Section 8.3), and/or alarms and occupancy sensors (Section 4.3).

6.4.3.3 Specifications and Features

There are a few specifications that are useful when planning or assessing the outdoor lighting levels of a school at night:

- For gates and doors where identification of persons and objects (e.g., packages, trucks) may take place, there should be illumination levels of at least 2 fc (per IESNA) (Reference 282). For reference, outdoors in full daylight is 1000 fc (Reference 338).
- For CCTV cameras, the minimum level of light is 0.5 fc for detection, 1 fc for recognition, and 2 fc for identification (Reference 4).

Table 6-6 presents the minimum recommended lighting levels for various parts of a school complex (Reference 282).

Table 6-6 Minimum Lighting Levels for Schools

School Area	fc
Outer perimeter	0.50
Vehicular entrances	10.0
Pedestrian entrances	5.0
Roadways	0.5 to 2.0
Open spaces	0.2
Open parking lot (low activity areas)	0.2
Open parking lot (high activity areas)	2.0

Additional specifications are as follows (Reference 282):

- The entire perimeter should be lit; cones of light on the perimeter should overlap.
- If there is a fence or wall, both sides should be lit.
- Lights should be directed down and away from the building to create glare for an intruder.
- Directed lighting should allow observation by a passerby or police officer.
- Protect the lighting system by installing protective covers over lamps, mounting lamps on high poles, burying power lines, and protecting switch boxes.
- If lights are automated, have a manual operation as a backup.
- The lighting should allow detection of human movement at 100 yards.
- Lights should be checked daily for operational status.
- Extra lighting should be installed at points of entry and points of possible intrusion.
- The power supply should be easily accessible.
- Lighting circuit drawings should be available to facilitate repairs.
- Switches and controls should be protected, weather-proof and tamper resistant, and accessible to security personnel.

6.4.3.4 Effectiveness

The research team did not find statistics on the effectiveness of outdoor security lighting on reducing violent crime in schools.

There is very little research comparing the effect of different kinds of outdoor lighting on crime levels. Some research suggests that adding security lighting in troubled neighborhoods reduces crime, but it is not specific to schools; in many cases, the crime simply moves to a nearby neighborhood (Reference 269). Interestingly, in the 1970s the San Antonio Public School System began leaving its school buildings and properties in the dark to reduce energy costs, but they also noticed a dramatic decrease in vandalism (Reference 303).

6.4.3.5 Policy Impacts

Some communities are voicing concern about light pollution contributing to sky glow. This spoils the natural effect of the night skies and increases power consumption. Any thoughtful school security lighting project should take light pollution into consideration (Reference 149). School security lighting projects should ensure they are compliant with local zoning codes with regard to light pollution.

6.4.4 CONCERNS ABOUT THE TECHNOLOGY

6.4.4.1 General Discussion (What It Does Not Do)

Lighting can aid in the detection of intruders or provide a deterrent to individuals trying to gain unauthorized access to the school building, but does nothing to prevent or slow physical access.

6.4.4.2 Vulnerabilities and Ways to Circumvent

As with indoor lighting, there are two potential vulnerabilities for indoor security lighting: tampering and loss of power. During an intentional or unintentional power failure, emergency lighting would be available, but security lighting typically would not be (Reference 282). Generators could be used to provide backup power to everyday school systems as well as security systems and lighting.

Another concern is that students or others with school access may tamper with light switches or automated sensors. These devices should be situated in such a way that minimizes tampering.

Students or others with access may tamper with Luminaires themselves. This is especially a concern for lighting for CCTVs. The location of lighting for CCTVs should be such that it is not easy to break the lamp, deface it, or render it inoperable. If a person were able to tamper with the CCTV light, the resulting video may not be usable for verification of a crime or for forensics.

6.4.4.3 Possibilities for Misuse

The author did not identify any likely misuses for outdoor lighting.

6.4.4.4 Liability and Safety Issues

Schools should carefully consider where outdoor safety lighting is most appropriate and consider whether increasing lighting in one area merely displaces crime to another less-lighted area.

6.4.4.5 Privacy Concerns

The authors did not identify any privacy concerns related to the use of outdoor lighting.

6.4.4.6 Accommodations for People with Disabilities

Switches should be accessible to people with disabilities.

6.4.4.7 Policy Concerns

Schools with existing programs to conserve energy may need to modify policies to allow the use of lighting during non-working hours. For example, if a school district has an existing policy to conserve energy by turning outdoor lights off at 10 pm, the security plan may call for security lighting to remain on until sunrise. This would have to be resolved at the district policy level.

6.4.5 COST CONSIDERATIONS

As previously discussed, the operating cost of incandescent lamps is the highest. Because of the high maintenance requirements associated with changing bulbs frequently and the high energy costs; this is not a desirable option for outdoor lighting. The maintenance costs for LEDs are the lowest, because the lamps last a very long time and therefore do not need to be changed as often. They also use the least

power. They are starting to be used on school campuses as exterior security lighting. For outdoor lighting, there is little need for training to operate or maintain lighting.

The formula to determine the cost to operate a light source is as follows (Reference 282):

$$\text{Watts} \times \text{Hours} = \text{Watts Hours}$$

$$\text{Watts Hours} \div 1000 = \text{Kilowatt Hours}$$

$$\text{Kilowatts Hours} \times \text{Cost of 1 kW per hour} = \text{Cost per Hour}$$

Table 6-7 (Reference 282) shows the operational costs over a 10-year period for one lamp of the most common outdoor lighting technologies. Additional cost impacts are noted in Table 6-8.

Table 6-7 Ten-Year Operational Costs of Commonly Deployed Outdoor Lighting Technologies*

Technology	Wattage	Lamp Changes	Energy	Maintenance	Materials	Cost of Operation
HPS	70 to 1000	3.7	\$927 to \$11,563	\$201	\$73 to \$224	\$1201 to \$11,988
LPS	35 to 180	4.9 to 5.5	\$629 to \$2308	\$268 to \$301	\$161 to \$345	\$1057 to \$2954
Metal halide	150 to 1000	5.8 to 8.8	\$1971 to \$11,248	\$321 to \$402	\$187 to \$365	\$2479 to \$12,014

*Based on 24 hours of on-time, 0.12 kW per hour, and \$55 per hour labor charge.

Table 6-8 Outdoor Security Lighting Cost Considerations

Cost Factor	Cost Description
Acquisition	Varies; identified products ranged from approximately \$73 to more than \$487 per lamp.
Installation	Can be significant if security lighting is not considered during construction. Potentially need to install infrastructure electrical wiring as well as fixtures, switches, sensors, and timers. Labor costs associated with the installation.
Operation and labor	Minimal (turn on switch if not automated)
User training	Little training required to operate or maintain lighting.
Maintenance	Minimal routine cleaning per manufacturer's instructions.
Consumables	Lamp bulbs need to be replaced. There is a wide range of bulb life. This is a cost driver.
Energy and energy dependency	Usually AC power; seldom DC (battery) power. Energy efficiency is a cost driver.
Software licenses	None
System integration	Can be integrated with motion sensors or set on timers. Can be integrated with backup generator power. Can be integrated with cameras, alarms, and sensors.

6.4.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

Outdoor security lighting is usually intended to reduce non-violent crimes such as vandalism, loitering, and burglary. Some research suggests that outdoor security lighting does little to prevent crime and may in fact increase crime (Reference 269). The school district of Clark County in Washington State saw a significant reduction in vandalism, loitering, graffiti, and burglary when they adopted a lights-out policy after 10:30 pm (Reference 149). As mentioned in Subsection 6.4.3.4, San Antonio schools also saw a significant reduction in vandalism costs when they turned their lights out at night. Therefore schools should discuss local crime trends with law enforcement when considering changes to security lighting.

6.4.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 6-9 presents examples of known vendors of outdoor lighting and motion sensors; however, it is not comprehensive and other vendors may exist. The list is current as of 4 September 2015.

Table 6-9 Outdoor Lighting Vendors

Vendor	Website	Notes
GE Lighting North America	http://www.gelighting.com/LightingWeb/na/solutions/outdoor-lighting/index.jsp	LED, HID
Lithonia Lighting	http://www.lithonia.com/pt/commercial+and+industrial+indoor/#.Vemc4KPD-AI	LED, metal halide, motion sensors
Grainger	http://www.grainger.com/category/ecatalog/N-/Ntt-Indoor+Lighting+Fixtures?cm_sp=CS_Banner-_-Lighting_L1_buckets-_-Indoor_Lighting	LED, HID, quartz halogen, motion sensors
Seesmart	http://www.seesmartled.com/product/ourproducts/	LED
Lighting Controls Association	http://lightingcontrolsassociation.org/about-lca/	Automated switching, occupancy sensor vendor lists
Williams	https://hewilliams.com/catalog/?brand=outdoor	LED, HID, CFL

6.5 CONCLUSION

This chapter covers lighting as it relates to violent crime prevention and detection in schools. In this context, it is referred to as security lighting. Security lighting can be installed internally (indoor) and externally (outdoor) to the school building. Generally, security lighting creates a deterrent to intrusion and enables other technologies, such as cameras, to work more effectively. Integration with other safety and security technologies (e.g., access control, surveillance systems, or cameras) may enhance or provide more robust school safety capabilities.

This page intentionally left blank.

Chapter 7. TECHNOLOGY REVIEW – SOFTWARE APPLICATIONS

Phillip R. Pratzner, MS; Subramaniam Kandaswamy, PhD; and Alexander G. Ihde, MS

7.1 INTRODUCTION

The use of information technology (IT) to enhance school safety presents two different challenges. First, school officials must consider how IT can best be applied to create a more effective security posture. Second, they must understand their students' digital presence to identify potential dangers the student and the school may face. This review addresses both of those challenges in the assessment of seven technologies:

- **Security planning tools:** Computer-assisted security plans, automation to create threat matrices, and decision support tools.
- **Physical security information management (PSIM):** A system for combining information from a variety of security technologies to create a common operating picture from the data.
- **Violence prediction software:** Data fusion technologies to predict potential trouble spots.
- **Visitor database checks:** Automated background and database checks for school visitors.
- **Mental and public health information sharing:** Collaboration software to provide information on individuals with dangerous mental health issues who may interact with students.
- **Social media monitoring and communication:** Systems to track student and community interactions on social media to provide early warning of potential bullying and crimes perpetrated by or to a school's population.
- **Tip lines:** An automated means for students, parents, and others to notify school officials of potential impending trouble.

Most of these technologies are intended to enable school staff to analyze and combine electronic data and resources to improve school safety. Only social media monitoring clearly provides situational awareness of students' digital presence, the second challenge, but many of these technologies at least indirectly address this challenge also. For instance, tip lines often serve as clues to threats discovered by students or community members on social media.

The common role for all of these technologies is detection and mitigation of security risk. They help identify risks in some cases, they assist in planning in other cases, and they enable the school or school district to recognize emerging security challenges in other cases.

It is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district prior to purchasing a safety or security technology. Table 7-1 presents the means by which the study team evaluated software application capabilities, aligned with the Federal Emergency Management Agency (FEMA) mission areas: Prevention, Protection, Mitigation, Response and Recovery.¹ This assessment combines the opinion of security subject matter experts and the informed judgment of the authors who evaluated the technologies. Reviewing this table provides a summary of the areas of school security and safety for which software applications may be best suited.

Table 7-1 Software Applications Impact on FEMA Mission Areas

Technology or Impact Area	Prevention	Protection	Mitigation	Response	Recovery
Security planning tool	MEDIUM Effective when findings are implemented, trained, and exercised	NONE No significant impact on protection was noted	MEDIUM Effective when findings are implemented, trained, and exercised	MEDIUM Effective when response actions are guided by the outputs of the tool	MEDIUM Effective when recovery actions are guided by the outputs of the tool

¹ The preparedness cycle consists of the following five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.
- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

Table 7-1 Software Applications Impact on FEMA Mission Areas (Continued)

Technology or Impact Area	Prevention	Protection	Mitigation	Response	Recovery
Physical security information management system	NONE No significant impact on prevention was noted	NONE No significant impact on protection was noted	HIGH Real-time monitoring can provide situational awareness for decision making	HIGH Real-time monitoring can provide situational awareness for decision making	HIGH Replay ability can provide situational awareness for decision making
Violence prediction software	CAUTION Immature technology. Has potential for high prevention impact	CAUTION Immature technology. Has potential for high protection impact	CAUTION Immature technology. Has potential for mitigation impact	NONE No significant impact on response was noted	NONE No significant impact on recovery was noted
Visitor database check	HIGH Identifies unauthorized individual before they can enter the school	HIGH Identifies unauthorized individual before they can enter the school	NONE No significant impact on mitigation was noted	NONE No significant impact on response was noted	MEDIUM May help during post-event investigation
Mental and public health information sharing	CAUTION Immature technology. Has potential for high prevention impact	CAUTION Immature technology. Has potential for high protection impact	CAUTION Immature technology. Has potential for mitigation impact	NONE No significant impact on response was noted	NONE No significant impact on recovery was noted
Social media monitoring and communication	HIGH Social media monitoring has the potential to identify otherwise unknown threats	HIGH Social media monitoring has the potential to identify otherwise unknown threats	NONE No significant impact on mitigation was noted	NONE No significant impact on response was noted	MEDIUM May help during post-event investigation
Tip line	HIGH Has the potential to identify otherwise unknown threats	HIGH Has the potential to identify otherwise unknown threats	NONE No significant impact on mitigation was noted	NONE No significant impact on response was noted	LOW May help during post-event investigation
<p>Impacts as they relate to a technology's ability to impact a school's ability to <i>prevent, protect, mitigate, respond, or recover</i> from an incident.</p> <p>High: Technology is expected to have a <i>significant</i> impact.</p> <p>Medium: Technology is expected to have <i>some</i> impact.</p> <p>Low: Technology is expected to have <i>little</i> impact.</p> <p>None: Technology is expected to have <i>no</i> impact.</p> <p>Caution: Technology will have an impact; however, it may also have unintended consequences.</p>					

Software applications are discussed in greater detail in Section 7.3.

7.2 UTILIZATION STATISTICS

The research team did not find utilization statistics common to all software applications. Relevant statistics applicable to security planning tools, social media monitoring, and tip lines are included in the Introduction section of each application. However, applicable statistics were not discovered for the sections on PSIM, violence prediction software, visitor database checks, and mental and public health information sharing.

7.3 SOFTWARE APPLICATIONS

7.3.1 SECURITY PLANNING TOOLS

7.3.1.1 Introduction

Across the nation, many schools and school districts have developed security plans; 88% of public schools have a written plan of procedures that addresses shootings or active shooters and 70% have drilled staff and students on use of this plan (Reference 237).

State laws mandate most of these plans today (see Chapter 12, Legal Review, for further discussion about state requirements), but many of them were originally developed in the aftermath of major school violence incidents, such as the Columbine shootings in 1999 (Reference 243). The focus, scope, and content of these plans vary widely, but there are numerous guides to developing an Emergency Operations Plan (EOP). For example, one resource (Reference 355) identifies planning principles and the six-step planning process advocated by the U.S. Department of Homeland Security (DHS) (Reference 362):

1. Form a Collaborative Planning Team: Composed of any department or office that is likely to impact or be impacted by emergency responses.
2. Understand the Situation: Consistently identifying threats and performing a risk assessment process to appreciate the unique environment of the school or schools.
3. Determine Goals and Objectives: Goals are broad, general statements that indicate the intended solution to problems identified by planners during the previous step, ensuring planners identify when major elements of the response are complete and when the operation is successful; Objectives are more specific and identifiable actions carried out during the operation, which lead to achieving response goals and determining the actions that participants in the operation must accomplish.
4. Plan Development (identifying courses of action): Generating, comparing, and selecting possible solutions for achieving the goals and objectives identified in Step 3; at least two options should always be considered in order to provide an adequate response, limiting damage to the affected population or environment.
5. Plan Preparation, Review, and Approval: Turns the results of course of action development into an EOP; the planning team develops a rough draft of the basic plan, functional annexes, hazard-specific annexes, or other parts of the plan as appropriate.
6. Plan Implementation and Maintenance: This must incorporate broad dissemination, training, exercising, assessing and an established process for periodic review and revision of the EOP.

The security planning or EOP development process must also address risk assessment (Reference 362). By assuming that the local police department provides information on risks in the surrounding

community, school officials can properly focus on their school community, particularly the vulnerabilities in the building, its occupants, and the immediate surrounding environment (Reference 355). The most successful assessments are conducted by a broad array of individuals, including support staff and first responders, and incorporate student, parent, disability, and location (urban, rural) issues (Reference 355). This is not a one-time activity because assessments will be used to develop the initial plan and to inform updates and revisions to the plan on an ongoing basis (Reference 355). In summary, an effective risk assessment must be thorough, inclusive, and “living” to the greatest extent possible.

FEMA provides a variety of risk assessment tools and other written guidance. Generally, these recommend the school or school district to affix scores to the probability, time, and consequences of a given hazard, and then determine the strategy to prevent, protect, or mitigate its impact (Reference 112). Because these are forms or written guidance, not a software solution, they provide a good example of what can be accomplished without technologies, and can help set priorities for schools that are considering how to use their technology budget. Another example is the Department of Education’s (DoED’s) vulnerability assessment process (Reference 356). Whatever the guide or checklist, and there are many, school officials should pick one that allows them to identify and analyze the range of hazards and risks they face in their school or school district.

The following terms and concepts are relevant to security planning tools as identified by the research team:

- **Risk assessment:** Entails understanding the likelihood that the specific threat or hazard will occur; the effects it will likely have, including the severity of the impact; the time the school will have to warn students and staff about the threat or hazard; and how long it may last (Reference 355).
- **Vulnerabilities:** Characteristics of the school (e.g., structure, equipment, IT or electrical systems, ground, and/or surrounding area) that could make it more susceptible to the identified threats and hazards (Reference 355).
- **EOP:** A written document, often accomplished at the school district level, that fulfills several functions (Reference 178):
 - Assigns responsibility to individuals within the organization for carrying out specific actions at projected times and places in an emergency
 - Sets forth lines of authority and organizational relationships
 - Shows how all actions will be coordinated
 - Describes how people and property will be protected in emergencies and disasters
 - Identifies personnel, equipment, facilities, supplies, and other resources available within the district or by agreement with other jurisdictions for use during response and recovery operations
 - Identifies steps to address mitigation concerns during response and recovery activities

7.3.1.2 How the Technology Is Used

The intent of electronic EOP tools is to guide school or district officials through a security planning process, enhancing knowledge of the specific school, its internal environment, and the surrounding community. Like manual EOP development, the process can build or strengthen relationships between school officials and local first responders and community groups. Discoveries made during the development process may suggest modifications of school policies. These tools also enable access to and dissemination of the EOP, and they provide an efficient method for updates to plans. Lastly, they

easily integrate with other tools and systems and provide EOPs in formats compatible with most common software like Adobe or Microsoft Word.

7.3.1.3 What Makes the Technology Good?

7.3.1.3.1 How the Technology Works

EOP tools and technologies facilitate the establishment and timely updating of EOPs. Presently, these tools are primarily available through state and DoED resources and represent a range of capabilities from actual EOP generation² to automated checklists to ensure a high quality EOP³ to simple online guides.^{4,5,6}

7.3.1.3.2 Differentiators

Technology and tools for school security planning can focus school officials on best practices for prevention, protection, mitigation, response, and recovery procedures. These can prepare staff and students for the actions necessary during an emergency by establishing teams, chains of command, and specific steps to take (Reference 147). The alternatives, security planning guides and books, rely more on manual input and written checklists that run the risk of becoming dated, thereby increasing the risk that key information is not included in the security plan.

7.3.1.3.3 Specifications and Features

Whether by generated by software, checklist, or consultant, a comprehensive EOP goes into detail and should incorporate and reflect most or all the following items⁷:

- Policies, procedures, emergency and crisis guidelines, and/or links to other safety-related documents
- Input from staff, students, parents and other members of the school community, as acquired by surveys or structured interviews
- Crime and discipline data
- Examination of physical facilities and grounds
- Analysis of related news, crime, and other information from public sources that may indicate how the community views the schools
- Review of crisis and other communications mechanisms, social media strategy, and related areas
- Examination and problem solving of safety concerns unique to a given school and school district

² U.S. DoED. *EOP ASSIST 2.0 Software: A Software Application for K-12 Schools, School Districts, and State Agencies*. Retrieved from <http://rems.ed.gov/EOPAssist.aspx>

³ Texas School Safety Center. *High-Quality Emergency Operations Plans*. Retrieved from https://rmt.txssc.txstate.edu/tools/hq-eop/assessment_questions

⁴ U.S. DoED. *Building Blocks to School Safety: A Toolkit for Schools and Districts for Developing High-Quality Emergency Operations Plans*. Retrieved from http://education.ky.gov/school/sdfs/Documents/Building%20Blocks%20to%20School%20Safety_A%20Toolkit%20for%20Schools%20and%20Districts.pdf

⁵ Florida Department of Education. *Safe Schools*. Retrieved from <http://www.fldoe.org/schools/safe-healthy-schools/safe-schools/index.shtml>

⁶ Center for Safe Schools. *Key Principles for School Security in Planning for Reductions in Force*. Retrieved from <http://www.safeschools.info/news/162-key-principles-for-school-security-in-planning-for-reductions-in-force>

⁷ National School Safety and Security Services. Retrieved from <http://www.schoolsecurity.org/school-safety-and-communications-services/school-safety-assessments/>

7.3.1.3.4 *Effectiveness*

An effective EOP tool has the following attributes:

- **Covers the range of hazards the school could encounter:** To ensure the school has an effective strategy to deal with relevant hazards (Reference 93).
- **Collects information required to deal with these hazards:** Whether this means prevention, protection, mitigation, response, or recovery from a given hazard, the EOP should be clear in how a school intends to address it.
- **Takes a systematic process, simplifying a highly complex undertaking:** For example, tax preparation software, such as TurboTax, breaks down something as complex as the U.S. Tax Code, issue by issue; an EOP tool or technology should do the same.
- **Prompts periodic review:** Whether the school is enhanced by new technology, the risk to the school has changed, or simply a predetermined length of time has elapsed, an effective EOP tool prompts the school officials that a change is necessary.

7.3.1.3.5 *Policy Impacts*

An EOP tool may be useful in addressing specific state and local mandates. However, selection and use of the tool itself should not prompt changes to existing policies and procedures.

7.3.1.4 *Concerns About the Technology*

7.3.1.4.1 *General Discussion (What It Does Not Do)*

Even an effective security planning or EOP tool or technology is not a failsafe for all potential security scenarios that a school might encounter. Such a tool can only cover those scenarios or conditions that school officials can imagine and specify. Therefore, if a school is presented with a situation that was not considered during EOP development, it may not be prepared to handle it.

7.3.1.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

EOP tools are vulnerable to operator error (e.g., entering wrong data) and hacking, which in theory could modify the plan itself. This is not a significant risk if hardcopies of the EOP are available when needed. However, if EOP access is maintained only electronically, heavy network traffic, interruption of power, or intentional hacking of the application could all prevent access to the plan when needed.

7.3.1.4.3 *Possibilities for Misuse*

If an individual interested in harming individuals is aware of specific vulnerabilities identified in the EOP associated with a given school, that person could use the information to evade security measures and increase the impact of a planned act of violence.

7.3.1.4.4 *Liability and Safety Concerns*

If done correctly, EOP tools and technologies normally help prevent liability and address safety concerns. However, if a given tool makes assumptions that cause school officials to skip or incompletely address key steps, safety could be compromised and the school could be liable.

7.3.1.4.5 Privacy Concerns

No specific privacy concerns were identified by the authors.

7.3.1.4.6 Accommodations Needed for Disabilities

An effective EOP tool must address the needs of students with disabilities during an emergency.

7.3.1.4.7 Other Issues

No additional issues were identified by the authors.

7.3.1.4.8 Policy Concerns

Because many states require by law that school districts have a comprehensive EOP and even specify items that need to be addressed (Reference 243), any EOP tool must be able to capture these legal requirements and ensure compliance.

7.3.1.5 Cost Considerations

In general, security planning tools are inexpensive or free (Table 7-2).

Table 7-2 Security Planning Tools Cost Considerations

Cost Factor	Cost Description
Acquisition	Purchase or service fees, particularly if using a consultant to complete the EOP or its associated risk assessment.
Exceptional installation costs	None, because in many cases this comes in a Software-as-a-Service (SaaS) format.
Personnel	The school district will require that selected personnel develop, maintain, and update the EOP.
Training	Whether by state officials, online or by consultants, there is a training cost to complete and maintain the EOP.
Maintenance	If using software on resident systems, updates and patches will be required.
Consumables	None
Energy and energy dependency	None
Software licenses	Although none specifically known, there are potential costs for acquiring licenses.
System integration	No known costs.

7.3.1.6 Emerging Technologies and Future Considerations

Future considerations can be linked to big data trends. For example, data fusion capabilities could automatically detect changes in crime data and even school disciplinary trends and prompt the appropriate school official to modify the EOP. Advances in data science could enable automated scanning of new school security practices, triggering an alert to prompt school officials to consider a change to their EOP. Although these capabilities are too costly for many school districts, prices for big

data capabilities continue to drop and are becoming commonplace on the Internet and with cloud technology environments.⁸

7.3.1.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 7-3 provides examples of known vendors of security planning services; however, it is not comprehensive and other vendors may exist. The list is current as of 21 October 2015.

Table 7-3 Security Planning Tools Vendors

Vendor	Website	Notes
National School Safety and Security Service	http://www.schoolsecurity.org/	EOP Appraisal
Safe Havens International, Inc.	http://safehavensinternational.org/	School Safety Assessment
Texas School Safety Center	https://rmt.txssc.txstate.edu/tools/hq-eop/assessment_questions	EOP Evaluation Software
U.S. DoED	http://rems.ed.gov/EOPAssist.aspx	EOP ASSIST 2.0

7.3.2 PHYSICAL SECURITY INFORMATION MANAGEMENT

7.3.2.1 Introduction

Because schools use a wide variety of school security technologies, each with its own purpose and reporting mechanism, it can be difficult for school officials to consume all of this information simultaneously and make sense of the information and its implications. PSIM is a unified system that ingests data from a variety of other security technology applications (such as an access control system, video cameras, and door sensors) to provide comprehensive situational awareness, enabling school officials to take timely actions (Reference 22). Integrated situational awareness is the primary benefit of PSIM. Built-in software tools and mechanisms within PSIM provide capabilities to the user to define rules for filtering and correlating relevant data. These rules may reference events, frequency, duration, times, and locations, depending on the information available and the needs of the school district.

For example, upon notification of an intruder threat from an access control system, PSIM can direct specific cameras in a video system to pan, tilt, or zoom in the area of intrusion and record the events (Reference 32). In addition, this real-time location information and video feed can be shared with law enforcement and other stakeholders. Systems integrated into PSIM still run in the background as independent systems while PSIM is extracting and aggregating data from all of these systems into a customized monitoring platform.

⁸ For example, Amazon Web Services serves as a platform for big data capabilities.

A complete PSIM software system has six key capabilities⁹:

- **Collection:** Device-independent software collects data from disparate security devices or systems.
- **Analysis:** Based on rules and filters, the software analyzes and correlates data, events, and alarms to identify real situations and their priority.
- **Verification:** The software presents situation information for an operator to verify.
- **Resolution:** The software provides standard operating procedures based on policies.
- **Reporting:** The software tracks information for compliance reporting, training, and, analysis.
- **Audit trail:** The software tracks operator interactions, records manual changes to security systems, and calculates reaction times for events.

It is difficult to estimate the prevalence of PSIM usage in K-12 schools. For security reasons, many schools do not disclose information about their situational awareness capabilities. However, literature indicates by anecdote that a number of schools currently use PSIM. For example, Littleton public schools in Colorado use a combination of security measures to ensure school safety including closed-circuit television (CCTV), motion detectors, proximity card readers, wireless duress system and security cameras, all integrated with PSIM.¹⁰

7.3.2.2 How the Technology Is Used

PSIM solutions can integrate security systems, such as access control systems, automated barriers, intrusion detection systems, lighting control systems, panic alarms, building management systems (such as power and heating), CCTV, fire detection, intercom, Internet Protocol (IP) phones, video analytics, geographic information system (GIS) mapping systems (Reference 55), and more. PSIM provides a common operating picture by presenting a single view from a central location (e.g., a district IT center), from different school locations, and/or from law enforcement field operations.

A PSIM system provides its users three outcomes (Reference 32):

- **Situational awareness:** PSIM sends information quickly when a system generates an alarm, along with prioritizing alarms. Additionally, it provides the user with a constant flow of information throughout an incident. For example, if a severe weather warning has been issued, the user can be constantly updated on how that weather event is progressing.
- **Situational management:** PSIM software analyzes triggering event data against digitized standard operating procedures and policies set by the stakeholders, organizes the presentation of relevant data, and applies filtering and correlation rules to determine whether the security threat is real or a false positive. Events and corresponding standard response procedures and controls are displayed. For instance, an option to lock down and/or activate a location-specific video recording might be available. Digitizing operating procedures helps ensure consistency in response protocols, regardless of the experience of the employee monitoring the PSIM system.
- **Situational reconstruction:** PSIM enables a comprehensive review of the incident after it happens by providing dates and times, when emergency responders arrived, what they did, and audio and video recordings. In this way, PSIM can be used for forensic analysis or reconstruction of the event to review procedures and explore ways to improve the response.

⁹ Systems Engineering, Inc. <http://www.seisecure.com/services/psim-integration/>

¹⁰ www.colorado.gov (February 2014) Tech Decisions Expert Series: *Choosing Technology for School Safety*.

7.3.2.3 What Makes the Technology Good?

7.3.2.3.1 How the Technology Works

PSIM provides a comprehensive overview of a school's current safety status by filtering useful information from multiple security systems. Significantly, PSIM primarily uses open source appropriate technology (OSAT). OSATs are designed as free and open source, with no intellectual property concerns, and can readily accommodate future and evolving technologies (Reference 267).

7.3.2.3.2 Differentiators

Often, there is difficulty distinguishing between PSIM and the integrated situational awareness capability provided by individual security systems, especially a video management system (VMS). In a VMS, video is the primary system; the other security systems provide data to the video through a single workflow. For example, if there is an intruder at a gate, the access control system sends an alarm and other related data to the video system through the integrated platform. However, to explore what caused the alarm and to execute further steps (such as determining whether a swipe card was used), the security staff would need to switch from the video system to the access management system (AMS) for the follow-up.

In contrast, PSIM has no primary system. It pools information, and multiple workflows, gathered from multiple security systems to provide a comprehensive overview of the current safety status (Reference 55). Thus, one system enables the user to examine data from the AMS and the VMS. PSIM systems have additional internal capabilities to outline and display predefined action plans usually not available in VMSs.

7.3.2.3.3 Specifications and Features

The most important specification for any PSIM system is that it integrates effectively—it must gather, process, and display information from diverse sources and systems (such as sensors and cameras). Integration protocols are therefore critical. Integration with third-party systems is easier if the subsystems support industry-accepted interoperability standards such as the Open Network Video Interface Forum (ONVIF). ONVIF is a global industry forum that facilitates the development of open standards for the interface of physical IP-based security products, such as how video surveillance and other physical security systems can communicate with each other. Such a standard enables integration of network cameras, server-based analytics engines, and access control systems. The vendor should provide a comprehensive list of the types of systems supported and integrated by the PSIM software, to include the following:

- Access control systems
- Automated barriers
- Intrusion detection systems
- Lighting control system
- Panic alarms
- Building management systems (such as heating)
- CCTV
- Fire detection
- Power and heating monitoring systems
- Intercom

- IP phones
- Video analytics
- GIS mapping systems

The PSIM interface must be appropriate for the technical skills and time constraints of the intended users and audience, including school administrators, law enforcement, medical responders, and fire departments. Ideally, the displays can be customized for the differing needs of these users so that each gets the information most relevant for their responsibilities.

Many features of PSIM vary with vendor providers. An overview of PSIM features and specifications is provided in five broad categories: procedural, data, visualization, event management, and group notifications. Table 7-4 provides details on features and their relevance to a PSIM system.

Table 7-4 PSIM Features and Specifications

	Procedural	Data	Visualization	Event Management	Group Notifications
Description	Rules-based solutions to manage increasing volumes of disparate systems (Reference 53)	Records, analyzes, and warehouses all disparate data sets, such as date and times of incidents, audio and visual recordings, weather alerts, etc. (Reference 32).	Graphical user interface allows user to select functions (Reference 218). Further, multiple and sophisticated map interfaces can allow objects and events to be tracked on a map (Reference 55).	Assists dispatch operations. Operators receive step-by-step guidance on what to look for, who to contact, how to respond, and when to escalate an incident (Reference 265).	Notifications provide contextualized data, unifying video, alarm and other sensor data, suited to a specific responder (Reference 161).
Key specific features	Customizable rules, event alert, dispatching, audit trail and history.	Correlations, announcements, and warnings .	Multi-layer mapping, real-time tracking, integrated video and events on map view.	Monitor systems and device state; alert responses mapped to policies, rules, and procedures; complete audit trails and reporting.	Email, Short Message Service (SMS)

Table 7-4 PSIM Features and Specifications (Continued)

	Procedural	Data	Visualization	Event Management	Group Notifications
Impact of Features	Provides digitization of standard operating procedures including steps to perform based upon events (Reference 32).	Ensures constant flow of information is available before, during, and after an incident. PSIM can repurpose data so departments and municipalities can share data (Reference 55).	Ensures end users receive relevant information for decision support.	Ensures proper responses to a host of events such as fire alarm notification, video cameras activated by intrusion alarms or duress buttons, HVAC and exhaust fans shut down or activated by other alarms (Reference 187).	Timely notifications and data are sent to appropriate responder in the necessary format to facilitate proper response.

7.3.2.3.4 Effectiveness

Several factors dictate the effectiveness of a PSIM system:

- The benefit of PSIM likely increases with the number of integrated systems.
- The selected PSIM product should be vendor and hardware agnostic to facilitate integrating existing and future systems.
- A PSIM system that supports sharing information in real time and taking collaborative actions with multiple incident responders (such as law enforcement) using various mobile devices provides significant capability in a crisis.

7.3.2.3.5 Policy Impacts

Employing PSIM enables coordination with local first responders (police and fire departments, specifically) to enhance their awareness and to synchronize, if possible, with their capabilities.

7.3.2.4 Concerns About the Technology

7.3.2.4.1 General Discussion (What It Does Not Do)

Because PSIM has no primary system, it can only pool information gathered from the multiple security systems to which it is connected. If one of those systems defaults or breaks, PSIM effectiveness is potentially degraded.

7.3.2.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Because the system is IP-based, PSIM may be vulnerable to cyber attack. The information security of a given system is highly vendor dependent.

7.3.2.4.3 *Possibilities for Misuse*

The insider threat is significant for misuse. PSIM depends on the skills of the security and information management team that maintains it. These persons, if ill intentioned, could prevent awareness of school officials of disruptive events, such as crime or intrusions.

7.3.2.4.4 *Liability and Safety Concerns*

False alarms and failure to alarm when needed can result if the parameter specifications in the rules engine or standard operating procedures are not carefully specified or if unforeseen events are misinterpreted by the predefined rules. This could cause liability and safety concerns to the school by delaying effective responses to security events.

7.3.2.4.5 *Privacy Concerns*

Because these systems aggregate data across multiple technologies, a more identifiable record of each individual is available. This, along with the intent to share PSIM displays with users outside of the school administration, such as emergency response personnel, increases the risk of a breach of student privacy. Policies and procedures should be drafted to address this possibility.

7.3.2.4.6 *Accommodations Needed for Disabilities*

The authors did not identify any disability accommodation issues.

7.3.2.4.7 *Other Issues*

The school district's network may have to be re-architected because live monitoring of video over the distributed architecture consumes significant bandwidth. Time synchronization between security technologies may be an issue for accurate monitoring and correlation of events in real time.

7.3.2.4.8 *Policy Concerns*

Depending on the school's policy about what type of information may be kept and for how long, PSIM trend and summary data analysis may be limited. Security personnel are in the best position to advocate for the optimal way PSIM can help a school official make effective policy decisions.

7.3.2.5 *Cost Considerations*

Cost of the total system for a typical installation is difficult to estimate because the divergent security systems incorporated into a PSIM system can vary from one school to another depending on security risk types and budget (Table 7-5). Costs also vary as a function of the chosen communication architecture (e.g., choosing between centralized or distributed architecture), the number and types of chosen security devices (e.g., surveillance cameras, door readers, intercoms), system integration, the number of servers, installation, software licenses, maintenance arrangements, and training.

Table 7-5 PSIM Cost Considerations

Cost Factor	Cost Description
Acquisition	PSIM is expensive. For example, the total cost of PSIM for the Littleton public schools in Colorado is about \$3 million, which is about 4% of the district's budget. ¹¹
Exceptional installation costs	The number of systems integrated will drive this.
Personnel	Either full-time personnel within the school district or vendors are required to run and maintain the architecture.
Training	Significant training will be required to configure and operate a PSIM system.
Maintenance	Routine maintenance and systems upgrades are required by PSIM.
Consumables	None
Energy and energy dependency	Minimal
Software licenses	License fees are standard.
System integration	The very purpose of PSIM is system integration, so these costs are not specific to this area, but rather embedded in PSIM acquisition costs.

7.3.2.6 Emerging Technologies and Future Considerations

Because new types of threats and attacks are emerging, any security system should also evolve to address the new security challenges. Emerging data analysis technologies for threat prediction is a desirable add-on to PSIM, which would transform the technology from a reactive to more proactive capability. The capability to select and filter the latest information from media broadcasts and social media to predict and prepare for potential dangers is the latest trend. VidSys and HP Autonomy announced a collaboration to develop a solution that combines VidSys' PSIM with HP's advanced information analytics platform.¹²

7.3.2.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 7-6 provides examples of known vendors of PSIM products; however it is not comprehensive and other vendors may exist. The list is current as of 13 October 2015.

¹¹ G. Grace, Director of Security and Emergency Planning, Littleton Public Schools. Interviewed on 23 July 2015.

¹² www.magal-s3.com/contentManagement/uploadedFiles/In_the_Press/a%26s-Understanding_Real_PSIM-Sep2014.pdf

Table 7-6 PSIM Vendors

Vendor	Website	Notes: Product Names
Aralia	http://www.aralia.co.uk/index.htm	Aralia PSIM
Bold Technologies	http://www.boldgroup.com/	Manitou PSIM
CNL	http://www.cnlsoftware.com/	IPSecurityCenter PSIM
Duos Technologies	http://www.duostechologies.com/	Centraco (PSIM Platform)
Fortem	http://fortem.com/	Omnipresence 3D Central Command
KapLogic	http://www.kaplogic.com/	Aegis
MerSecurity	http://www.mersecurity.com/	Secure-M PSIM
Pantascene	http://www.pantascene.com/	Vistascene, Sensorscene, Intelliscene
Priority5	http://www.priority5.com/	Touch Assisted Command and Control System (TACCS)
Proximex	http://www.proximex.com/	Surveillint
Prysm	http://www.prysm.com/	AppVision
PureTech Systems, Inc.	http://www.puretechsystems.com/	PureActiv
SENTEL Corporation	http://www.sentel.com/	Remote Delay Relay (RDR) and RDR Command Post
Software House	http://www.swhouse.com/	C-CURE 9000
SureView Systems	http://www.sureviewsystems.com/	Immix
Verint Systems	http://www.verint.com/	Verint Situation Management Center PSIM; Nextiva PSIM
VidSys	http://www.vidsys.com/	VidSys PSIM

7.3.3 VIOLENCE PREDICTION SOFTWARE

7.3.3.1 Introduction

With close attention being given to school violence, school officials and behavioral health specialists seek to identify such threats before they arise. One technology under consideration is software that predicts violent behavior in individuals or groups, allowing school staff to intervene before significant problems arise. Police forces are exploring the use of violence prediction software to forecast gang violence (Reference 298) and to assist in allocating resources to prevent crimes through targeted police presence (Reference 127). Studies have been conducted to predict violent behavior in behavioral health patients (Reference 224) and within the Department of Defense (Reference 85). While no violence prediction software designed specifically for schools was identified, these existing tools offer the potential for technology that allows schools to mitigate or prevent violent behavior before it happens.

7.3.3.2 How the Technology Is Used

Violence prediction software is currently used by certain police departments as a forecast tool. Police using these systems are cued to potential crime locations or, in some cases, at-risk persons. This information enables police to redistribute their resources to deter the predicted crimes or put officers in position to answer anticipated calls more quickly. In the case where specific individuals are identified, police may use that information as local law and procedures permit.

7.3.3.3 Concerns About This technology

Violence prediction software does not predict all incidents of violent behavior, and school officials should not expect it to provide sufficient warning to obviate other security measures. Specifically, the authors identified three primary vulnerabilities of this software:

- **False alarms:** The software may key on social media and behavioral history and generate an alert when no violent behavior is planned. Recommended uses and specifications for this type of software must allow users to review raw data, especially from social media, to assess whether an intervention or an escalated security posture is appropriate. Repeated false alarms may cause a loss of confidence in the software or improper focus on non-threatening individuals.
- **Hacking:** This software is vulnerable to cyber attack. Sophisticated hackers may also be able to spoof the software by generating activity that could trigger false alarms.
- **Training requirements:** Data generated from this software require trained analysts to review the data and make sound judgments.

The authors also identified two challenges that present potential liability and safety concerns, both closely related:

- **Expectation of security:** Public awareness of the existence of a violence prediction system will bring with it an expectation that threats will be identified and reported before violence occurs, which may expose the school to additional liability if a crime does occur.
- **Lowered vigilance:** The presence and knowledge of this software may cause some students and community members to believe that reporting suspicious behavior by other means is not necessary, resulting in fewer tips and less vigilance. Existence and operation of the software does not guarantee safety, or even the identification of all potential threats. It remains the responsibility of human operators to communicate the knowledge of threats appropriately.
- **Perception of negligence:** In the event that the system predicts a threat and later a criminal act occurs, there is significant risk that the school could be accused of negligence for failing to prevent the crime.

7.3.3.4 Emerging Technologies and Future Considerations

Although research in this area is growing, models available for general use are limited and tools appropriate for school use are not yet established. Most such tools focus on predicting the location and perpetrators of likely violence within a city, with some offering “street level granularity” (Reference 325) in their forecasts. These existing tools offer the potential for schools to monitor external community trends that could affect their internal populations and in the future might be modified to focus on a school campus instead of a city.

7.3.3.5 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 7-7 provides examples of known vendors of Violence Prediction software; however, it is not comprehensive and other vendors may exist. The list is current as of 15 November 2015.

Table 7-7 Violence Prediction Software Vendors

Vendor/Provider	Website	Notes
PredPol	http://www.predpol.com/	Currently oriented to police
Accenture	https://www.accenture.com/us-en	Used by the London Metropolitan Police
Social Analysis and Intelligence Group	http://saig-llc.com/	Product: Second Sight
PAR	http://www4.parinc.com/Default.aspx	Product: Classification of Violence Risk (COVR)

7.3.4 VISITOR DATABASE CHECKS

7.3.4.1 Introduction

In addition to logging in visitors on paper or electronically, many schools are increasingly incorporating technology for visitor database checks. By using a visitor's driver's license or other state-issued identification, these systems can potentially screen for registered sex offenders, domestic dispute offenders, and other individuals of interest, etc. This process can happen "in just a few seconds" (Reference 193). If a potential threat is identified, administrators and/or law enforcement are alerted and the individual can be denied entry to the school or be escorted off the property, depending on the school's policy. This technology has been associated with several security best practices (Reference 147). Figure 7-1 depicts the various components of a visitor database system, where a typical system comprises a scanner, printer, and display screen.

**Figure 7-1 Various Components of a Visitor Database System**

Definitions relevant to this technology include:

- **National Sex Offender Public Website: (NSOPW):** First established in 2005 as the National Sex Offender Public Registry, the NSOPW is the only U.S. Government website that links public state, territorial, and tribal sex offender registries in one national search site, and it presents the most up-to-date information provided by each source. Information is hosted by each jurisdiction, not by the NSOPW or the Federal Government, because there is no Federal registry for sex offenders due to different legal standards within jurisdictions at the state and local levels.¹³
- **Self-service kiosk:** A small standalone device providing information and services on a computer screen.¹⁴
- **Real-time information:** Information is presented, discovered, or visualized based upon current data.¹⁵ An example would be a request of the NSOPW returning real-time results rather than checking a locally maintained database where data is not up to date.

7.3.4.2 How the Technology Is Used

The central purpose of visitor database checks is to prevent unwelcome people from entering the school. Without a way to check offender databases, a school must rely on the staff member who greets visitors to determine whether to allow a visitor to enter the school or not. This might mean consulting a list of individuals to whom parents have authorized the school to release the student. However, this can be time consuming or inaccurate if, for instance, a custody issue arises and the release form is not updated. In addition, it does not preclude the possibility that a parent is a registered sex offender who should be denied entry to school grounds. Some systems can link in to court records as well. Using a visitor database check helps to validate the identity of people requesting entry by requiring an official form of identification and to verify they are not on a database of recognized threats.

7.3.4.3 What Makes the Technology Good?

7.3.4.3.1 How the Technology Works

There are two primary options for how a school operates this technology. In the first, the school assigns a staff member to run the software and perform associated administrative functions. The advantage of this method is that the individual can verify that the presented identification (ID) matches the visitor and can screen the purpose of his/her visit. The staff member can then print a time stamped badge with a photograph, name, and reason for visit and areas of the school the visitor is authorized to access (Reference 193).

The second option for schools is the self-service kiosk. Visitors typically use a touch-screen to enter their own information. Just like a system administered by district staff, kiosks can take photos, scan driver's licenses, run instant background checks, and deny access to sex offenders, non-custodial parents, or other individuals who have no legitimate reason for being in the school (Reference 193). According to the president of LobbyGuard Visitor Management Solutions, a kiosk company, there is typically one kiosk per school, and "many schools are introducing two-door systems, where a visitor enters a vestibule through an unlocked door. The kiosk is in the vestibule, and after the visitor's information is verified by the kiosk, a front desk staff member can buzz them through the second, locked door into the school" (Reference 193).

¹³ U.S. Department of Justice. "About NSOPW." Retrieved from <http://www.nsopw.gov/en/Home/About>

¹⁴ Merriam-Webster definition of kiosk. Retrieved from <http://www.merriam-webster.com/dictionary/kiosk>

¹⁵ Merriam-Webster definition of real time. Retrieved from <http://www.merriam-webster.com/dictionary/real-time>

In addition to a computer with an Internet connection, additional hardware, such as optical scanners, badge paper, and ink, is required by these systems. With certain visitor database check systems, consumables will only be available from the prime vendor, making pricing uncompetitive. School officials often may have other options provided by the vendor, such as unique badges with fading or color-changing ink to prevent reuse (Reference 193). Even with these customizations, vendors claim software installation is simple and a single school can typically start screening within days.^{16,17}

7.3.4.3.2 *Differentiators*

One alternative to this system is a background check conducted by a school resource officer. These background checks can be recorded in a manner discoverable to other school officials and potentially incorporated into a local visitor database system (one that does not check sex offender registries in real time), but this would have to be a manual effort. Visitor background check technologies conduct a check against the same databases every time, and most of them have recording features that enable a person's visit history to be referenced and known at any moment.

7.3.4.3.3 *Specifications and Features*

The authors identified specifications that may distinguish vendors:

- **Accuracy:** The system must be able to confirm the visitor is neither a sex offender nor has custodial issues with a student; a false positive—flagging a parent with no sex offender or custodial issues—could increase tension between parents and the school faculty or result in a loss of confidence in the system.
- **Speed:** The faster the system can perform a check, the better the school can manage visitors. Vendor literature¹⁸ identifies speed as a primary consideration for choosing a system.
- **User friendliness:** The system must be intuitive and easy to use, especially for visitor kiosk systems.

Other optional features and enhanced functionality for this technology also should be considered. One such feature allows users to add notes to visitors' files or designate guests by type. For example, grandparents can be listed as qualified to pick up a student, whereas noncustodial parents are barred from buildings (Reference 193). Some vendors provide visitor database checks as part of a fully integrated school check-in system for visitors, staff, and students. In addition to the visitor status check, these systems can tie in disparate data sources that fulfill administrative needs, such as tardy student tracking, approved student pick-up and early dismissal tracking, and faculty check-in and check-out. Lastly, some vendors offer schools improved ability to account for non-security-related visitor tracking, such as parent volunteer hours, important for both school officials and Parent Teacher Association (PTA) officers alike.

7.3.4.3.4 *Effectiveness*

Although it rarely happens, visitor background check technologies have stopped unauthorized individuals from entering schools (Reference 195). No empirical evidence supports the assertion that the

¹⁶ Raptor Technologies, LLC (2015) Retrieved from <http://www.raptorware.com/>

¹⁷ Hall Pass (2015) "Hall Pass Solutions." Retrieved from <http://www.hallpassid.com/>

¹⁸ Raptor Technologies, LLC (2015), Hall Pass (2015), Lobby Guard (2015), KeepnTrack (2015), Fast Pass (2015), and School Gate Guardian (2015)

technology acts as a deterrent, but many school administrators have expressed that the technology contributes to better school security (References 195 and 326).

7.3.4.3.5 Policy Impacts

Implementation of visitor background checks requires that schools have a robust policy on processing visitors who have backgrounds, such as placement on a sex offender registry, that alert the system. For example, the policy might include an option to escort the visitor. The legality of accessing and using such databases may vary by jurisdiction and should be considered when developing the requirements for a system.

7.3.4.4 Concerns About the Technology

7.3.4.4.1 General Discussion (What It Does Not Do)

Visitor background checks perform a fairly limited function. Although many specific vendor systems do this very well, they are generally expensive. In addition, because they are connected to the Internet, there must be access and sufficient bandwidth for the school to perform a database check. Depending on the school district and volume of visitors, this may present a challenge, as capacity may be limited. Lastly, a school may be required to plan for multi-lingual support, which is not supported by all vendors.¹⁹

7.3.4.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Although the technology does generally have security controls, as with any software that connects to the Internet, it is vulnerable to cyber attack.

7.3.4.4.3 Possibilities for Misuse

An individual with sufficient access, knowledge, and permissions could intentionally enter data (through normal means, not hacking) that deny a visitor access to the school. The authors consider this highly unlikely, but the potential exists given the right data permissions and policy gaps.

7.3.4.4.4 Liability and Safety Concerns

Under certain conditions, this technology could create large queues, increasing the possibility of a safety concern, especially in a vestibule kiosk. Accordingly, vendor systems must scale to handle large numbers of visitors to accommodate activities on school grounds that are open to the community, such as sporting events, school plays, or graduation ceremonies or alternate accommodations must be made.

7.3.4.4.5 Privacy Concerns

Some parents, custodians, and civil liberty groups have concerns about the technology flagging individuals for transgressions in their distant past that would require them to be escorted through the school (Reference 295). There are additional concerns that school officials may use visitor ID to view other court records. This perspective is perhaps best summed up in this way (from Reference 195):

Parents, members of the public, and even school board members expressed concern that instead of keeping students safe, the system would become a deterrent to parent

¹⁹ Lobby Guard (2015) and KeepnTrack (2015)

involvement for individuals who are undocumented, have pasts they want to put behind them or who worry about personal information being collected and stored by the school.

Therefore, schools must balance these concerns with the potential added benefit of security provided by visitor database checks. Significantly, despite this challenge, an ever-growing number of school districts and schools have chosen to implement visitor database checks (Reference 147).

7.3.4.4.6 Accommodations Needed for Disabilities

Because self-service kiosks are best combined with a vestibule system, school officials must ensure the vestibule and tool meet Americans with Disabilities Act compliance. Consideration for individuals using a wheelchair as well as those who have difficulty or are visually impaired should be incorporated. Clear procedures are required, and must be incorporated early in the design planning process.

7.3.4.4.7 Other Issues

No additional issues were identified by the authors.

7.3.4.4.8 Policy Concerns

The effectiveness of this technology is dependent, at least in part, on the school or school district's policy on data use and storage. Additionally, policy on handling data (e.g., who may access it, how long it is kept, what type of data is archived) will all need to be addressed. Policy must allow school officials to keep these kind of data so as to use visitor background check technologies to their full advantage.

7.3.4.5 Cost Considerations

Because this is expensive technology, schools and school districts should carefully consider the associated costs of the various vendors (Table 7-8).

Table 7-8 Visitor Database Checks Cost Considerations

Cost Factor	Cost Description
Acquisition	Basic systems normally include a check for registered sex offenders, and possibly a screen for individuals with restraining orders or custody issues; systems that are more elaborate will screen for suspended or expelled students, known gang members, or for any custom alert. More expensive systems from the same vendor could include a detailed criminal background check. Driver's license scanners, a badge printer, and badges will often be included in the base price of the system. This technology can be an expensive proposition for a large school district: one district spent \$294,500 for a 186-campus district (Reference 326).
Exceptional installation costs	Self-service kiosks often have a high initial installation cost. A vestibule is highly desirable with a kiosk; if one does not exist, the cost of building one should be factored in. Additional accessories, normally not required, include a camera, a color badge printer, and color-coded badges. If background checks are unacceptably slow because of a lack of bandwidth, a school might have to purchase additional Internet capacity. A vendor should be able to readily supply the bandwidth required to operate their systems.
Personnel	Unless fully automated, the system will require some staff operation during all school hours.

Table 7-8 Visitor Database Checks Cost Considerations (Continued)

Cost Factor	Cost Description
Training	Training is minimal for most systems; the addition of a system, however, may require training related to new policies.
Maintenance	Scanners, badge printers, and cameras require routine maintenance. Software patches and updates are required as well.
Consumables	Blank badges and ink.
Energy and energy dependency	Increased energy demands related to use of this software should be negligible.
Software licenses	Per seat or computer license fees are not common with this technology.
System integration	No known costs.

7.3.4.6 Emerging Technologies and Future Considerations

Perhaps the most relevant emerging factor regarding visitor background checks is its increased adoption. Although there are concerns that could constrain the growth of visitor database checks, this is becoming commonplace technology in schools (Reference 147).

A significant future consideration is the integration or fusion of this technology with other data sources. Current integration efforts focus on check-in systems, tying visitor database checks with tardy student tracking, approved student pick-up, early dismissal tracking, and faculty check-in and check-out. In the future, a fully integrated system might include all check-in systems, as well as volunteer hours, social media monitoring, and student ID scanning, to identify just a few data sources.

7.3.4.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 7-9 provides examples of known vendors of visitor database checks; however, it is not comprehensive and other vendors may exist. The list is current as of 21 October 2015.

Table 7-9 Visitor Database Checks Vendors

Vendor	Website	Notes
Hall Pass	http://www.hallpassid.com/	Visitor Background Check System
KeepnTrack	http://www.keepntrack.com/	Visitor Background Check System
LobbyGuard	http://lobbyguard.com/	Visitor Background Check System-Kiosk
Raptor Technologies, LLC	http://www.raptortech.com/	Visitor Background Check System
School Gate Guardian	http://www.schoolgateguardian.com/	Visitor Background Check System
Sisco Identification Solutions	http://www.siscocorp.com/Products/fastpass.aspx	Visitor Background Check System: Fast-Pass

7.3.5 MENTAL AND PUBLIC HEALTH INFORMATION SHARING

7.3.5.1 Introduction

After the attack at Sandy Hook Elementary School, concern about individuals with mental illness conducting violent acts came to the forefront as a significant consideration for school security. However, this concern has not developed into formal technological systems that share information about threats to schools posed by individuals with mental illnesses. Although general information sharing needs have been documented in many different forms, the need has not been addressed for schools and mental health.

The concept for a mental health information sharing system is outlined in the Substance Abuse and Mental Health Services Agency (SAMHSA) Behavioral Health Medicaid Information Technology Architecture (BH-MITA) Concept of Operations document (Reference 296), which communicates a vision for future capabilities required for the agency:

A seamless and transparent integration of treatment programs and recovery support services across not just health related entities, but across other sectors as well, such as the courts system, housing and employment services, correctional institutions and probation offices, the child welfare system, social services and disability, and any other systems and services that impact individual health and wellness.

Although this description comes from a mature vision statement, the study team did not find specific technologies already in use dedicated to sharing mental health information, especially regarding threats of violence. It is expected that specific concerns identified by healthcare professionals would be communicated directly to law enforcement, and specific individuals who are threatened should be warned by whatever means of communication are legally justifiable to mental health practitioners and public safety officers.

Mental or behavioral health information sharing should provide warning of threats perceived by behavioral health practitioners, such as psychiatrists, therapists, or social workers, directly to law enforcement agencies at local, state, and Federal levels, as appropriate. The information would include patient identifying information and some notion of the nature of the threat presented by the patient, including:

- Likelihood of the patient carrying out a violent act as described
- Expected means by which the violent attack will be conducted, including knowledge of the patient's ownership of weapons or other means to perpetrate a violent attack
- Specific individuals or generic organizations mentioned by the patient as targets for violence

Information would be provided as a "push" directly to law enforcement agencies in jurisdictions in which the patient lives, works, and attends community events (such as sports leagues or church gatherings) and where people who share a close relationship with the patient reside. The sharing technology should also facilitate use of tip lines (see Subsection 7.3.7) to provide another avenue by which the threat information is communicated.

7.3.5.2 Policy Impacts

A mental and public health information sharing technology would force the school district or school to develop a policy on sharing the data. School counselors in particular would have to know the policy well to fully implement the advantages this technology offers.

7.3.5.3 Privacy Concerns

By their nature, these systems report details of a patient's identity and the fact that the patient is undergoing behavioral health treatment, thereby invoking Health Insurance Portability and Accountability Act (HIPAA) Security Rule requirements.²⁰ Because personal information is shared, privacy concerns must also be addressed for the policies of the state in which the system operates.

As schools and school districts consider how to improve safety in the future, it is inevitable they will consider how to improve awareness of all possible threats. The willingness to monitor social media, a controversial activity, supports this assertion. In the same way, school districts will consider how they can use and share mental and public health data. If other similar activities serve as a guide, the beginning of this activity will likely be modest.

7.3.6 SOCIAL MEDIA MONITORING AND COMMUNICATION

7.3.6.1 Introduction

Social media has created a challenge for parents and schools to keep their kids safe online. Schools are increasingly confronting the issue by considering whether to monitor students' online interactions to protect them from dangers such as bullying and awareness of drug use, violence, and thoughts of suicide (Reference 378). "We have to go where our children are," says Gary Margolis, a retired police officer and president of Social Sentinel, a social media monitoring company, "and our children are in two places now—in the schools and in the digital space." (Reference 141)

Relevant statistics confirm this assertion:

- Student digital presence (Reference 201)
 - For many teens, texting is their dominant communication method. Some 88% of teens text their friends at least occasionally, and 55% do so daily.
 - Along with texting, teens are incorporating a number of other devices, communication platforms, and online venues into their interactions with friends, including:
 - Instant messaging: 79% of all teens instant message their friends; 27% daily.
 - Social media: 72% of all teens spend time with friends via social media; 23% daily.
 - Email: 64% of all teens use email with friends; 6% daily.
 - Video chat: 59% of all teens video chat with their friends; 7% video chat daily.
 - Video games: 52% of all teens spend time with friends playing video games; 13% play daily.
 - Messaging applications (apps): 42% of all teens spend time with friends on messaging apps such as Kik and WhatsApp; 14% every day.

²⁰ <http://www.hhs.gov/ocr/privacy/>

- Bullying in schools (Reference 58)
 - 19.6% of students reported being bullied on school property and 14.8% reported being bullied electronically in the 12 months before the survey.

While social media monitoring technology is credited with an ever-growing list of threats averted or resolved (References 141 and 378), it is not without significant policy, parental, and even legal challenges. In other contexts, what social media monitoring provides is called *intelligence* (Reference 351) although school officials would probably use the term *understanding*. Schools generally regard data from social media monitoring as an extension of the information and tips gathered through personal conversations or anonymous tip lines.

Several definitions and concepts are important to social media monitoring:

- **Social media:** Forms of electronic communication, such as Web sites for social networking and microblogging, through which users create online communities to share information, ideas, personal messages, and other content (e.g., videos).²¹ Examples of social media include Facebook, Twitter, Google+, Wikipedia, LinkedIn, Reddit, and Pinterest.²²
- **Geofencing:** A geofence is a virtual barrier. Software programs use global positioning system or radio frequency ID features embedded into information systems, including mobile devices, to define geographical boundaries. Programs that incorporate geo-fencing allow an administrator to set up triggers to send an alert when a device enters (or exits) the boundaries defined by the administrator.²³
- **SaaS:** A software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.²⁴

7.3.6.2 How the Technology Is Used

Social media monitoring technology employs tools “to proactively prevent, intervene and [watch] situations that may impact students and staff.” (Reference 141) School officials use specified alerts from software that monitors Facebook, Twitter, Snapchat, and other social media to determine whether action is required to, for example, prevent a suicide, stop bullying, or protect students from other possible violence. This essentially extends school security into cyberspace, where students spend a significant amount of their time.

7.3.6.3 What Makes the Technology Good?

7.3.6.3.1 How the Technology Works

The school officials either set up the monitoring themselves or contract it as a service from a third-party vendor who is responsible for both the monitoring and the notification of trusted officials in the school. The basic concept is as follows:

- The specific capability tracks social media accounts (by name and/or geographic area) for certain keywords. School officials may ask parents and students for additional keywords to add to the watch list of terms for scanning.

²¹ Merriam-Webster definition of social media. Retrieved from <http://www.merriam-webster.com/dictionary/social%20media>.

²² TechTarget. “WhatIs.com” Retrieved from <http://whatIs.techtarget.com/definition/social-media>.

²³ TechTarget. “WhatIs.com” Retrieved from <http://whatIs.techtarget.com/definition/geofencing>.

²⁴ TechTarget. “WhatIs.com” Retrieved from <http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service>.

- If a monitored keyword is used, the post will be read to check for the potential threat it is tied to, such as violence, bullying or harassment, drug or alcohol use, weapons possession, or other threats.
- Threats are forwarded to school officials and police if necessary.

7.3.6.3.2 *Differentiators*

Few competing technologies enable a broad picture view of social media monitoring. This is primarily because no locally created software can scale effectively to scan the amount of social media that covers students' digital lives. A "homegrown solution" might include locally produced code that could scan school computer systems but little else. Additionally, administrators could manually review social media for troubling posts from their students, but this is time consuming and not comprehensive.

Recruiting community involvement and implementing a tip line is one low-cost alternative that could address parts of this challenge, allowing students and parents to report potential threats found on social media. However, if the school or school district wants to understand a broader picture consistently rather than rely on this type of reporting, social media monitoring offers significant capabilities.

7.3.6.3.3 *Specifications and Features*

The authors identified several features to distinguish social media monitoring tools:

- **User friendliness:** The capability must be easy to use and provide actionable information to the school official. Additionally, the more clear and concise the reports, the easier it is for the school official to identify a problem.
- **Timeliness of reporting to school officials:** Information that the technology reveals on social media should be passed to the appropriate user as quickly as possible. Currently, social media monitoring is best used for detecting potential threats, cueing school or law enforcement personnel to investigate. Because the investigation is not automated, the humans performing it need as much time as possible to gather all social media and other information to determine a course of action.
- **Trends analysis:** The social media monitoring capability must be able to spot trends such as increased bullying or drug use in certain locations. Trend analysis enables school officials to address a problem sooner rather than later.
- **Customization:** The evolution of slang can be very localized. The software must accept new terms, phrases, and acronyms as they become associated with threats.

7.3.6.3.4 *Effectiveness*

Many school districts assert that social media monitoring has prevented suicides and stopped bullying (References 141 and 378). In the summer of 2012, the Glendale school district in suburban Los Angeles, working with a social media monitoring firm, identified a student who was talking on social media about "ending his life." "We were able to save a life," said Richard Sheehan, the Glendale superintendent, adding that two students in the school district had committed suicide the past two years (Reference 378).

7.3.6.3.5 *Policy Impacts*

Implementing this technology necessarily requires accumulating previously unavailable sensitive information on students. Social media monitoring vendors suggest that the information being accessed

has been posted to an online forum and is therefore not subject to the same restrictions as private information, however the legality of accessing social media should be investigated.

Policies should be in place to determine what action is appropriate if a threat is identified, particularly whether students, parents or the community should be notified of a potential threat.

Additionally, policy on handling data (e.g., who may access it, how long it is kept, what type of data is archived) will need to be addressed. Further, schools must decide what range of threats they will look for with this technology, including dealing with false or vindictive information streams.

7.3.6.4 Concerns About the Technology

7.3.6.4.1 General Discussion (What It Does Not Do)

This technology has great potential to provide awareness of criminal activities or safety concerns that many schools would find useful. However, social media data are not definitive, and just because a threat is (or is not) revealed on social media does not mean it is (or is not) present or capable of happening in the future.²⁵

7.3.6.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Social media monitoring takes place in the public space; therefore, students can decide to keep everything private (e.g., correspondence, posts) and discuss or plan dangerous activities in ways that are unmonitored.

7.3.6.4.3 Possibilities for Misuse

An unscrupulous or overzealous third party or school official could violate the privacy of a student for behavior not related to a security concern, such as complaining about a teacher or school policy. Spurious threats that may overwhelm school officials and law enforcement are also a potential concern.

7.3.6.4.4 Liability and Safety Concerns

It is critical to understand the legal definitions of public and private information. In some cases, which are rare and within the law in certain states, school districts accessed private accounts. This has normally been associated with bullying or suicide issues (Reference 378).

A school may face liability concerns when it investigates or addresses a threat. Making threatening comments on social media does not necessarily mean that the individual truly intends to follow through, and may not be considered a criminal act. Therefore, care must be taken to protect private information during the investigation of a threat and any subsequent preventative actions.

In the event that the system identifies a potential threat which ultimately results in a criminal act, there is significant risk that the school could be accused of negligence in failing to prevent the act.

7.3.6.4.5 Privacy Concerns

There are significant privacy concerns because students and parents likely expect any conversations that take place outside of school remain outside of school jurisdiction, even when held on public domains.

²⁵ A thorough discussion of this dilemma, focused on the U.S. Intelligence Community, is covered in D. Rumsfeld's *Known and Unknown: A Memoir* from Penguin Books (2011).

Schools that have decided to conduct social media monitoring have made a judgment on the limits of school officials' authority. "There is no expectation of privacy. That is the policy," Jackson Schools Technology Director David Proffitt said. "Anything that creates a significant disruption to teaching or learning is our business." (Reference 103)

7.3.6.4.6 Accommodations Needed for Disabilities

The authors did not identify any disability accommodation issues.

7.3.6.4.7 Other Issues

No additional issues were identified by the authors.

7.3.6.4.8 Policy Concerns

Even the basic act of social media monitoring—not looking at closed conversations but rather monitoring only the public domain—is legally challenging for school districts. As to the use of social media monitoring, Daniel Domenech, executive director of the American Association of School Administrators, the school superintendents association, has said it is "not always clear" legally what can be done and what is within the scope of the district's authority (Reference 378). "In one state, the court will support the district and say, 'absolutely, you have the right to do that.' In a very similar situation in another court, the court will rule 'absolutely not, it's freedom of speech,'" Domenech said. "So the whole legal issue right now is very much up in the air."

7.3.6.5 Cost Considerations

Although the costs are straightforward, social media monitoring can be costly, depending on the size of the school district (Table 7-10).

Table 7-10 Social Media Monitoring Cost Considerations

Cost Factor	Cost Description
Acquisition	Initial cost ranges from \$9,000 to more than \$40,000, depending on the size of the school district (References 61, 103, and 378)
Exceptional installation costs	None
Personnel	For SaaS capabilities, the designated individuals must assess notifications generated by this technology; however, if a third-party vendor assesses notifications, no school personnel are needed. Once a notification is deemed worthy of an intervention, school or local law enforcement resources are needed.
Training	Training is required for staff on how to effectively assess notifications.
Maintenance	Frequent revisions of key words. Normal software patches and updates are required for SaaS products.
Consumables	None
Energy and energy dependency	Increased energy demands related to use of this software should be negligible.
Software licenses	One- to three-year licenses are the norm.
System integration	This system is normally a standalone capability.

7.3.6.6 Emerging Technologies and Future Considerations

Like visitor background checks, perhaps the most relevant emerging factor regarding social media monitoring and communication is its increased adoption. Despite the policy concerns that could constrain its growth, school districts are interested in this technology.

Future considerations will involve the ever-shifting public sentiment on privacy, such as where the public domain starts and stops. Accordingly, schools that conduct social media monitoring will likely not receive universal support in the future, and will need to maintain constant awareness of law, policy, and school population sentiments on the subject.

7.3.6.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 7-11 provides examples of known vendors of social media monitoring and communications. It is not comprehensive and other vendors may exist. The list is current as of 21 October 2015.

Table 7-11 Social Media Monitoring Vendors

Vendor	Website	Notes
CompuGuardian	http://www.compuguardian.com/	School computer monitoring
Geo Listening	https://geolistening.com/schools/	Social media monitoring
Media Sonar Technologies	http://www.mediasonar.com	Social media monitoring
Snaptrends	http://snaptrends.com/	Social media monitoring
Social Sentinel	http://www.socialsentinel.com/	Social media monitoring

7.3.7 TIP LINES

7.3.7.1 Introduction

A 2004 report by the U.S. Secret Service and U.S. DoED concluded that in 30 of the 37 school attacks that occurred between 1974 and 2000, at least one person had information that the attacker was thinking about or planning the school attack (81%). In 22 incidents, more than one person had information about the attack before it occurred (59%). In 28 of the 30 cases where someone knew, that person was a peer—a friend, schoolmate, or sibling (93%). “Some peers knew exactly what the attacker planned to do; others knew something ‘big’ or ‘bad’ was going to happen, and in several cases knew the time and date it was to occur. An adult had information about the idea or plan in only two cases.” (Reference 375) The purpose of tip lines is to bring this information forward before an incident occurs.

With regard to tip lines, during the 2013–2014 school year, 47% of public schools reported having a structured, anonymous threat reporting system in place. In addition, the larger the school, the more likely it was to have a threat reporting system. For example, in schools with 300 students or less, 36% had the capability; for those with 1000 students or more, 61% had the capability (Reference 237).

7.3.7.2 How the Technology Is Used

Tip lines provide a safe, confidential way for students to alert authorities about information that may be useful in preventing school attacks, bullying, and suicidal behaviors. Tip lines are not new; police and local government officials have long understood their value. They were widely used after the 1999

shootings at Colorado’s Columbine High School, and received renewed interest from a handful of states and districts that sought to strengthen violence-prevention efforts following the 2012 shootings at Sandy Hook (Reference 33).

Anonymity has been shown to be a critical consideration for school-age children. They do not want to be known as a “snitch” and show a greater willingness to report when they can remain anonymous (Reference 33). A rare exception to this is discussed in Subsection 7.3.7.3.3, but in general, anonymity must be a guiding concept. Tip lines fall into two categories: voice (telephone call) or electronic (email, text, or smartphone app).

Acquiring and implementing a tip line is relatively simple. A school or district decides on a vendor, acquires or purchases the tool, or it is provided for free by state entities such as the local department of education, then publicizes the capability. Schools and school districts will usually put up posters and then distribute brochures, cards, emails, and texts to ensure all parties know what vendor or method they are using and give general instructions on how to provide a tip.

7.3.7.3 What Makes the Technology Good?

7.3.7.3.1 How the Technology Works

Tip lines work through four basic steps. First, a student, parent, or other interested party who is aware of an issue submits a tip via phone, email, text, or app, frequently to a third party (a vendor). Second, the third party contacts the tipster, performing case management and obtaining all the pertinent information and details. Once all relevant information has been gathered, the third party reports the issue to trusted school officials or, if necessary, local law enforcement. Lastly, school officials work with the third party to determine the appropriate individuals to contact as required by school policy.

Schools must consider the means of communication (telephone, email, text, or app, or combination thereof), the mode of interaction between the tipster (questions they are asked, visualization of the screen, etc.) and the third-party provider, and the interface between school officials and the third-party provider (e.g., reports, information elements received, statistics, alerts). See Figure 7-2.

- **Voice tip lines** should be used only for reporting non-emergency events. Tipsters commonly use voice tip lines for reporting crimes related to weapons, violence, threats, property damage, and thefts. Calls are free and can be made from a pay phone, cell phone, home phone, or school phone. Callers are not required to give their name, and the tip line calls should not have the caller ID feature activated.

Tips are usually provided by parents, teachers, school administrators, students, and other concerned citizens. The majority of the calls originate from parents. As vendors report, “nearly 70% of our calls originate from concerned parents,”²⁶ and “the majority of hotline calls (over 90%) are from parents who are concerned about bullying at their child’s school.”²⁷ Calls from parents are likely to be genuine (i.e., not prank calls) and are more comprehensive.

- With **electronic tip lines**, as with voice tip lines, the tipster initiates the process by reporting an unsafe or suspicious activity, almost always anonymously. The tipster then receives, if he/she requests, a confidential auto response that the message has been received and how further

²⁶ The Safe School Help Line (2015) Retrieved from <http://www.schoolhelpline.com/implement.html>.

²⁷ Hodges, J. (2015) Program Specialist, Georgia Department of Education. *Safe and Drug-Free Schools*. Email to S. Kandaswamy, 4 September 2015.

contact will be conducted. For the text option, this information is normally obtained through two-way text chat. If a tipster has pictures or video, he/she receives instructions for sending this information. Once all of the information is gathered, an email, text, or other type of alert is sent to the designated school administrator, including a recap of the actual conversation the third party had with the tipster, along with pictures or video if they were provided. If the situation is life threatening, a special alert, often a text message, can be sent to the administrator's cell phone. As with all tip lines, the school administrator must investigate the report and determine the appropriate follow-up action.

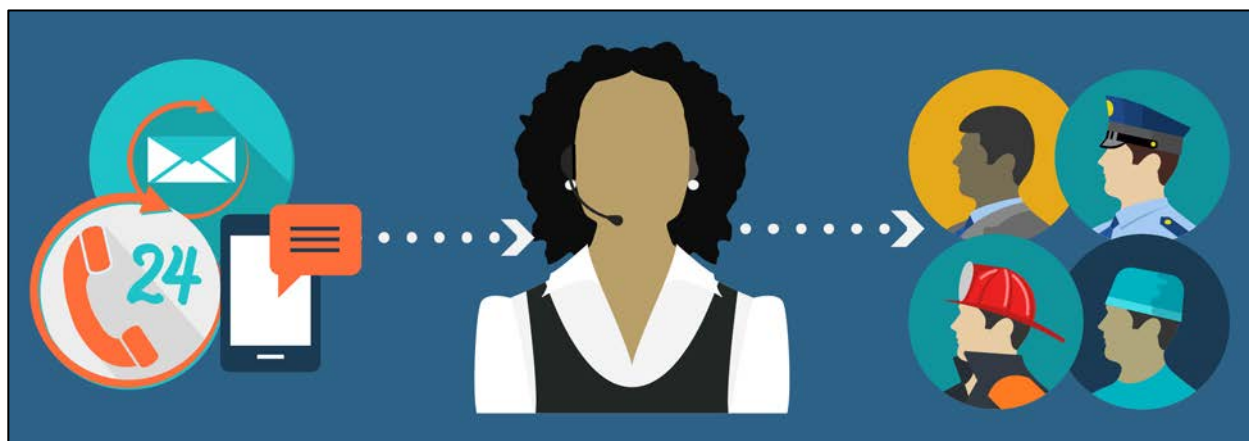


Figure 7-2 How Tip Lines Work

7.3.7.3.2 Differentiators

Tip lines provide schools with a low-cost alternative to social media monitoring to address essentially the same issues—bullying, suicide, and criminal activities. Tip lines require active participation by a tipster, whereas social media monitoring collects information passively; however, schools can still gain significant awareness of potential threats, especially when they tailor the tip method to the media the students commonly use, such as texting. Additionally, because participation is voluntary, tip lines do not have the same policy and legal issues challenges as social media monitoring.

7.3.7.3.3 Specifications and Features

The authors identified several features that distinguish one vendor and/or provider from another:

- **Reachability:** For voice, this is measured as the success rate for reaching a live agent, operator, or dispatcher on the first try without the call being blocked or the caller receiving a busy tone. For electronic tip lines, reachability includes the tipster success rate for contacting and receiving confirmation that the tip was received.
- **User friendliness:** The tip line must be easy to use and not present any challenge for the user whether using voice or electronic format.
- **Timeliness and accuracy of reporting to school officials:** Third-party providers should pass tips to the appropriate officials as soon as they can verify the content and context of the tip. In emergency situations, timeliness may supersede rigorous verification.
- **Timely resolution by school officials.** Tracking the timespan between the time the third party contacts the school and the resolution time for the situation can indicate how quickly the school

officials respond and the thoroughness and accuracy of the information passed from the third party.

- **Anonymity, as appropriate:** The general rule is that the tipster must remain anonymous. However, if the tipster is suicidal or making specific threats, policy should indicate that the tip line provider is able to identify the tipster to school officials and law enforcement.

7.3.7.3.4 Effectiveness

Tip lines have helped to prevent suicides, stop bullying, and confiscate weapons.²⁸ Although they rely on individuals reporting the tip, they have proven a cost-effective service for a schools intent on improving their security.

7.3.7.3.5 Policy Impacts

The authors identified three policy impacts for this technology which should be explored for compliance with state and local regulations:

- **Third-party questions:** What questions should the third party be allowed to ask?
- **Third-party use of information:** What can the third party do with the information it receives from tipsters after the incident has been addressed or resolved? Where do they keep it? How long is the information stored?
- **Follow-up policy:** Does the school address every issue from the tip line? How do they address fallacious or vindictive tips?

7.3.7.4 Concerns About the Technology

7.3.7.4.1 General Discussion (What It Does Not Do)

Tip lines must have individuals willing to provide tips. Students in particular are sometimes reticent to report, and usually will only report if they are sure the information will remain confidential (Reference 33). The larger the pool of people involved, the higher the odds that useful information will be discovered. The size of the community may also affect the effective anonymity. In a small community callers may be more reluctant to call because their identity may be readily guessed from the information provided.

7.3.7.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Tipsters must know that their identities are protected. While it is possible that someone could hack into a tip line database, humans are the most likely source of a breach of confidentiality. Caution must be taken to protect tipster identities when investigating reports. If the tip line appears to report the tipster's name to school officials, the integrity of the program may be questioned by the student population even if that name was not released. By policy and agreement with the school district, the third party can, with rare exception, report a suicidal case to officials, where the safety of the tipster takes precedence over the need for anonymity.

7.3.7.4.3 Possibilities for Misuse

The reporting of tips that deliberately contain false information is a concern. This is not so much a specific fault of the technology, but rather with policies on how the false information is handled. There

²⁸ School Tip Line. Retrieved from <http://www.schooltipline.com/>.

are no easy ways to address false reporting, other than the due diligence of a tip line third party to verify some basic facts, such as whether a certain student is in a particular school.

7.3.7.4.4 *Liability and Safety Concerns*

No immediate liability or safety concerns were identified.

7.3.7.4.5 *Privacy Concerns*

The primary privacy concern for tip lines is for tipsters. They must be convinced they can report in a confidential manner.

7.3.7.4.6 *Accommodations Needed for Disabilities*

For individuals with a hearing or speech impediment, a voice tip line may be ineffective without specific measures to address these issues. Likewise, without accommodation, an electronic tip line requiring reading may be ineffective for individuals who are visually impaired. Voice and electronic tip lines should support the use of assistive technologies.

7.3.7.4.7 *Other Issues*

The only low-cost alternative to a professionally developed tip line is an organic, school- or school-district-run program where existing faculty or district officials check a tip line (perhaps a message machine or complaint box) and follow-up as required. This presumes schools and school districts have the capacity and skills to investigate and follow up on tips appropriately. In addition, by using local school officials, anonymity, a major benefit of a third party, may be denied to the tipster, whether by perception or in reality.

7.3.7.4.8 *Policy Concerns*

If school officials do not allow tip lines to be anonymous, they are far less likely to be used and consequently are less effective.

7.3.7.5 *Cost Considerations*

Tip lines are very cost effective, as detailed in Table 7-12.

Table 7-12 Tip Line Cost Considerations

Cost Factor	Cost Description
Acquisition	Basic tip lines scale well, and are often mandated and bought in bulk, whether at the state or school district level. For the most part, this is an inexpensive technology; there is no software or hardware to buy. As discussed, in some cases this is a free service provided by state departments of education. In other cases, however, there might be subscription fees for monthly reports.
Exceptional Installation Costs	None. There are potential advertising costs, if not provided by the vendor as part of the service.
Personnel	With purchase of a tip line capability, the third party provides the personnel necessary to employ the service.
Training	The only training required is delivered through the tip line posters and information sheets, normally from the vendors.

Table 7-12 Tip Line Cost Considerations (Continued)

Cost Factor	Cost Description
Maintenance	Some service costs may be required to provide and install updates.
Consumables	None.
Energy and Energy Dependency	Increased energy demands related to use of this software should be negligible.
Software Licenses	None.
System Integration	No known costs.

7.3.7.6 Emerging Technologies and Future Considerations

Tip lines typically work best when they employ the technology most commonly used by students. If most students communicate by texting daily, that is the tip line medium likely to be most effective. All evidence points to an increase in electronic tip lines, primarily text at this time, until another medium gains wide use by students. Smartphone tip line apps are starting to appear, and are likely to become more common as well.²⁹

7.3.7.7 Current Vendors

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 7-13 provides examples of known vendors of tip lines; however it is not comprehensive and other vendors may exist. The list is current as of 21 October 2015.

Table 7-13 Tip Line Vendors

Vendor	Website or Phone Number	Notes
CyberBully Hotline	http://www.cyberbullyhotline.com/	Text or call formats; anonymous
School Tip Line	http://www.schooltipline.com/	Email or text formats; anonymous
Safe2Tell	http://safe2tell.org/	Call format; anonymous
Text 2 Stop It	http://www.text2stopit.org/	Text format; anonymous
reportit	www.reportit.com	For-profit call format
SafeschoolHelpline	www.schoolhelpline.com	For-profit call format
Anne Arundel County Public Schools	877-676-9854	No-cost call tip line provider
Georgia Department of Education and Department of Public Safety	877-SAY-STOP	No-cost call tip line provider
Ionia Public Schools Community, Michigan	800-815-TIPS	No-cost call tip line provider
Kansas School Safety Hotline	866-748-7047	No-cost call tip line provider

²⁹ <http://safe2tell.org/>

Table 7-13 Tip Line Vendors (Continued)

Vendor	Website or Phone Number	Notes
Missouri School Violence Hotline	866-748-7047	No-cost call tip line provider
Ohio Safer Schools Tip Line	877-644-6338	No-cost call tip line provider
Rolla Public Schools Safety Hotline	573-458-0115	No-cost call tip line provider
West Virginia Safe Schools Helpline	866-SAFE-WVA	No-cost call tip line provider

7.4 CONCLUSION

The common theme for software applications is the detection and mitigation of security risk. These applications and capabilities enable school staff to analyze and combine electronic data and resources. Software applications generally have the potential to help school staff prevent, mitigate, and recover from acts of criminal violence; they are not as effective in protecting against it in the manner that a physical barrier (e.g., locked door, gate, or fence) might.

The authors draw one other significant conclusion. All of these capabilities provide the school and school officials with situational awareness. In this way, school officials mitigate and even lower risks with a combination of these capabilities. Many factors have to be weighed in this investment—including cost, unique school demographics and environment, and expected effectiveness in a given school district—but these capabilities are increasingly more relevant to the total picture of school security.

Chapter 8. TECHNOLOGY REVIEW – SURVEILLANCE

John Cristion, MS; Morgan F. Gaither, MS; Subramaniam Kandaswamy, PhD; Lauren A. Brush, MS; and Alexander G. Ihde, MS

8.1 INTRODUCTION

Violent episodes in American schools in the past decade have influenced educators, legislators, parents, and concerned citizens to prioritize school safety in their communities and consider the inclusion of surveillance in their safety plans. Surveillance measures may include stationing security officers in school buildings or implementing surveillance technologies such as video cameras, gunshot detection systems, global positioning system (GPS) technology, and more.

The following four surveillance technologies are investigated further in this chapter:

- **Surveillance cameras** in schools are used to monitor students, school staff, school grounds, and school assets. Additionally, these systems are used to identify visitors, deter crime, and investigate crimes that have been committed. Surveillance cameras are often considered less expensive and a better solution than devoting staff resources to monitor specific access points and higher-risk areas such as stairways and hallways.
- **Gunshot detection technology** is used to detect a gunshot, identify the gunshot's location, and immediately send an alert to 911 operators and first responders (e.g., local police, fire, or ambulance), and notify the school staff. The technology can use an acoustic sensor alone or with optical sensors to detect gunshots. Some gunshot detection systems automatically trigger security cameras near the sensors to zoom in on (and record) the direction where the gunshot was detected to capture real-time information on the shooter and the environment.
- **Location tracking technologies** like radio frequency identification (RFID) systems and GPS can be used to track students and school buses.
- **Unmanned aerial vehicles (UAVs)** are often fitted with surveillance cameras and may provide a capability to remotely monitor school grounds in a more mobile manner than traditionally mounted cameras.

It is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district prior to purchasing a safety or security technology. Table 8-1 presents the means by which the study team evaluated surveillance capabilities, aligned with the Federal Emergency Management Agency (FEMA) mission areas: Prevention, Protection, Mitigation, Response and Recovery.¹ This assessment combines the opinion of security subject matter experts and the informed judgment of the authors who evaluated the technologies. Reviewing this table provides a summary of the areas of school security and safety for which surveillance systems may be best suited.

Table 8-1 Surveillance Systems – Technology Impact Summary

Surveillance Systems	Prevention	Protection	Mitigation	Response	Recovery
Cameras					
Security camera	LOW Awareness of security cameras may discourage security threats and violence	LOW Awareness of security cameras may discourage security threats and violence	NONE No significant impact on mitigation was noted	MEDIUM When monitored, can expedite response from security staff, law enforcement, etc.	MEDIUM Information may help during post event investigation

¹ The preparedness cycle consists of the following five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.
- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

Table 8-1 Surveillance Systems – Technology Impact Summary (Continued)

Surveillance Systems	Prevention	Protection	Mitigation	Response	Recovery
Acoustic Systems					
Gunshot location system	NONE No significant impact on prevention was noted	NONE No significant impact on protection was noted	NONE No significant impact on mitigation was noted	LOW May shorten first responders' reaction times	NONE No significant impact on recovery noted
Tracking Systems					
Student location system	NONE No significant impact on prevention was noted	NONE No significant impact on protection was noted	NONE No significant impact on mitigation was noted	HIGH May enable location of students	LOW May have some forensic use in reconstructing where students have been
Vehicle location system	NONE No significant impact on prevention was noted	NONE No significant impact on protection was noted	NONE No significant impact on mitigation was noted	HIGH May enable location of buses	LOW May have some forensic use in reconstructing where buses have been
Remote Surveillance					
UAV	NONE No significant impact on prevention was noted	NONE No significant impact on protection was noted	NONE No significant impact on mitigation was noted	MEDIUM When flown, can expedite response from security staff, law enforcement, etc.	LOW Information may help during post-event investigation
<p>Impacts as they relate to a technology's ability to impact a school's ability to <i>prevent, protect, mitigate, respond, or recover</i> from an incident.</p> <p>High: Technology is expected to have a <i>significant</i> impact.</p> <p>Medium: Technology is expected to have <i>some</i> impact.</p> <p>Low: Technology is expected to have <i>little</i> impact.</p> <p>None: Technology is expected to have <i>no</i> impact.</p> <p>Caution: Technology will have an impact; however, it may also have unintended consequences.</p>					

Surveillance systems technology is discussed in greater detail in Sections 8.3 to 8.6.

8.2 UTILIZATION STATISTICS

The authors did not find empirical data related to gunshot detection, location systems, or UAVs when used for school safety. This section provides a brief description and explanation on the available utilization statistics for the use of security cameras. Figure 8-1 depicts security camera utilization data from Table 20.1 in Reference 236.

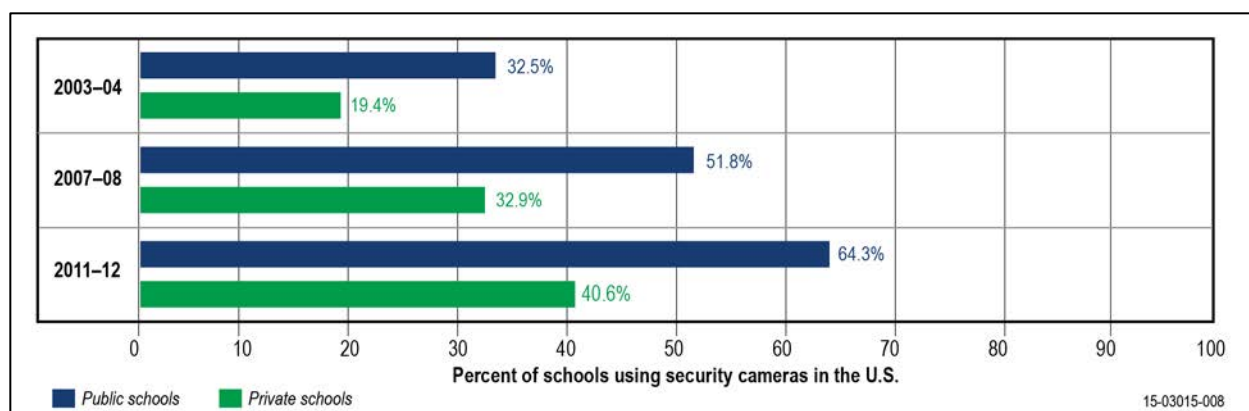


Figure 8-1 Security Cameras Usage and Trending in Combined, Public, and Private Schools

Two general conclusions can be made based on the data:

- Cameras are deployed in a higher percentage of public schools than private schools.
- Irrespective of the type of school, the use of cameras in schools steadily increased from 2003 through 2012.

8.3 SURVEILLANCE CAMERAS

8.3.1 INTRODUCTION

Public and private schools deploy thousands of security cameras; this technology is the second most-used security measure (Reference 354) in public schools.² In general, video camera signals are classified by their method of delivering video signals:

- **Analog** cameras convert the video signal into a format that can be received by equipment such as televisions (TVs), video cassette recorders (VCRs), or monitors.
- **Digital or Internet Protocol (IP)** cameras (also known as network cameras or cameras with an IP connection) have video signals that are digitized and transported over a network.

Both analog and digital cameras can transmit their images using wired or wireless connections. The bandwidth can be compressed, making the transmission and utilization very efficient.

The video feed provided by a surveillance camera is typically linked to a digital system for monitoring, recording, and archiving. Feeds from these cameras can be monitored locally or at central monitoring stations such as remote school district administrative offices or local law enforcement agencies. Additionally, surveillance cameras can be integrated with or contain video analytics software to increase monitoring capabilities.

² In both public and private schools, controlling access to school buildings during school hours was the number one safety or security measure used. In private schools, enforcing a strict dress code, wearing uniforms, and controlling access to school grounds preceded camera deployment in importance.

8.3.2 HOW THE TECHNOLOGY IS USED

Camera systems may be employed in a variety of ways. In its simplest form, a camera system consists of one or more video cameras, a monitor, and a recorder. Their value to security is heavily dependent on the way they are deployed, the degree to which their operation is integrated with other security systems, and how they are used by school staff. Three common ways camera systems are used, along with their associated benefits, are described next.

8.3.2.1.1 *Monitored Cameras*

In this configuration, camera feeds are transmitted to a monitor with an individual assigned to watch the video feed. Staff should be provided regular breaks to maintain the ability to effectively monitor the camera feeds. “According to some industry research, an operator can only monitor about eight screens at one time. After only 12 minutes of continuous video monitoring, an operator will often miss 45% of activity, and after only 22 minutes of continuous video monitoring, an operator will often miss 95% of activity.”³ The benefit of operating cameras in this fashion is that when a behavior is observed, security staff immediately can be sent to the location of the incident immediately.

8.3.2.1.2 *Unmonitored Cameras*

In this configuration, the camera’s video feed is transmitted to a monitor that does not have a dedicated observer. This includes systems where the monitor is located in a school office or on an administrative assistant’s desk, where the staff member has a primary duty other than observing the monitor. These systems, where observation is only occasional, may have value in deterring undesirable behavior in students, but only limited value in response or mitigation. Stored video footage may aid in identifying perpetrators and verifying testimony, making it valuable for forensic analysis as part of the recovery process.

Many schools install cameras to monitor the main entrance. In this configuration, when a visitor approaches the entrance, he or she must press a doorbell that prompts office staff to look at a monitor and take appropriate action.

8.3.2.1.3 *Smart Cameras*

Although smart cameras, or systems employing video analytics capabilities, can be monitored or unmonitored, video analytics provides automatic detection and alerting features. These systems apply software algorithms to a digital video feed. Based on the algorithms’ outputs, predetermined responses are implemented. Using video analytics, the feeds from hundreds of cameras may be filtered so that the highest priority inputs are given special attention. For example, the system may be capable of detecting a suspicious package or a person in a prone position in a hallway, prompting that video feed to be highlighted for further observation by security staff so that they can select an appropriate response.

Video analytics processing may be conducted anywhere with a high-speed Internet connection. Most schools cannot afford security staff dedicated 100% to video monitoring. Video analytics allows this function to be centralized across multiple schools (e.g., at the district level), enabling the dedicated observer to initiate contact with school staff or law enforcement, as appropriate. Staff at the affected school may be cued to observe the video themselves to enhance their situational awareness and coordinate a response.

³ <http://www.securitymagazine.com/articles/82771-video-surveillance--see-it-now--see-it-later--or-go-both-ways>

8.3.3 WHAT MAKES THE TECHNOLOGY GOOD?

8.3.3.1 How the Technology Works

8.3.3.1.1 Analog Cameras

Analog cameras are the original video recording mode. They produce a signal that can be received by a TV, VCR, or a monitor. They transmit signals either wirelessly or through wired connections such as coaxial cables to a storage system. Traditionally, with analog cameras, one or more dedicated individuals are assigned to watch several monitors or review recordings.

8.3.3.1.2 Digital Cameras

Digital cameras record images or video in digital form. Unlike traditional analog cameras that record on film or tape, digital cameras record on a hard disk, flash memory card, or digital video disk (DVD). As with all digital devices, there is a fixed maximum image resolution. Images are often transferred to a computer with a universal serial bus (USB) cable, a memory card, or via wireless transmission.

8.3.3.1.3 Basic Analog Closed-Circuit Television (CCTV) System

More than 30 years ago, most cameras were analog and used VCRs to record video feeds. The term *closed circuit* is used to draw a distinction from broadcast television. CCTV is primarily used for surveillance and security purposes. Signals from the cameras are transmitted to a limited set of monitors and recorders and are not intended for public distribution. Systems typically included the cameras to transmit a video signal from a remote location, a quad or multiplexer to allow the users to select which videos to be shown on monitors or recorded, a VCR to record the video signal, and a monitor to observe the video. Figure 8-2 displays typical equipment used in an analog CCTV system. Common limitations associated with analog CCTV systems include scalability (e.g., adding more video feeds) and the need to change video tapes frequently, although newer digital storage systems can alleviate this limitation.

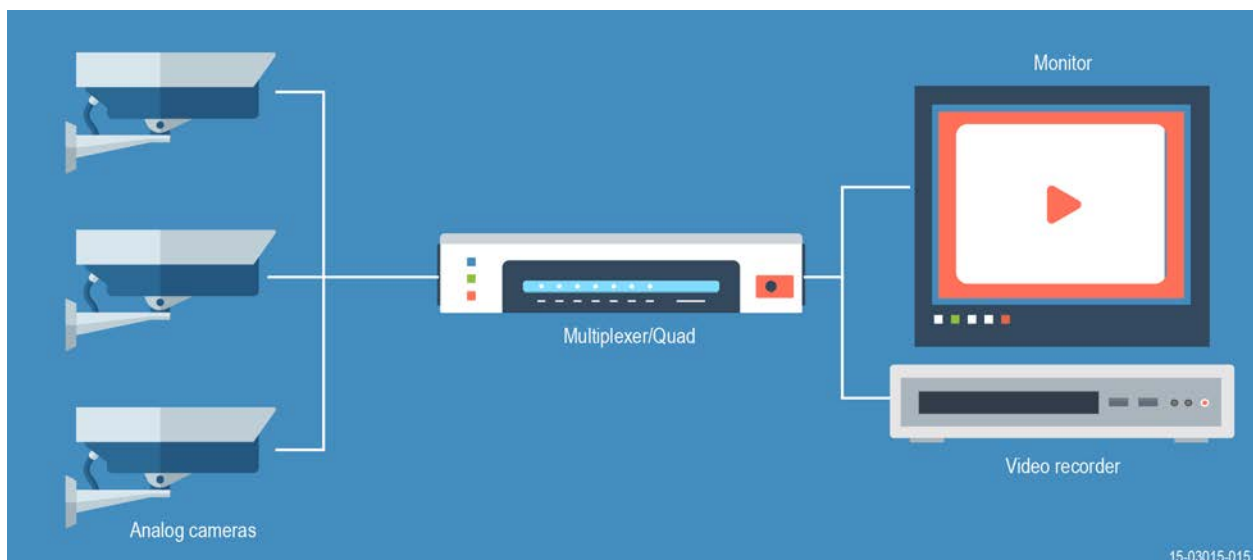


Figure 8-2 Analog CCTV System

8.3.3.1.4 Basic Digital CCTV System

Digital video recorders (DVRs) replaced VCRs in the mid-1990s. By providing the functionality of the quads and multiplexers and the VCR, the DVR simplified the CCTV system and also supports up to 32 camera ports per DVR box, but several boxes may be grouped together to allow more camera ports. Added benefits of using DVRs include the capability to quickly search and access video feeds of interest.

8.3.3.1.5 IP or Network System Cameras

An IP camera is another type of video camera commonly employed for surveillance. It can send and receive data via a computer network and the Internet. The terms *IP cameras* and *network cameras* are used interchangeably in the literature. The system is end-to-end digital (no analog components are involved). The digitized video is transported over the local area network (LAN) to a server or computer housing the video management software. Figure 8-3 displays typical equipment used in an IP camera system.

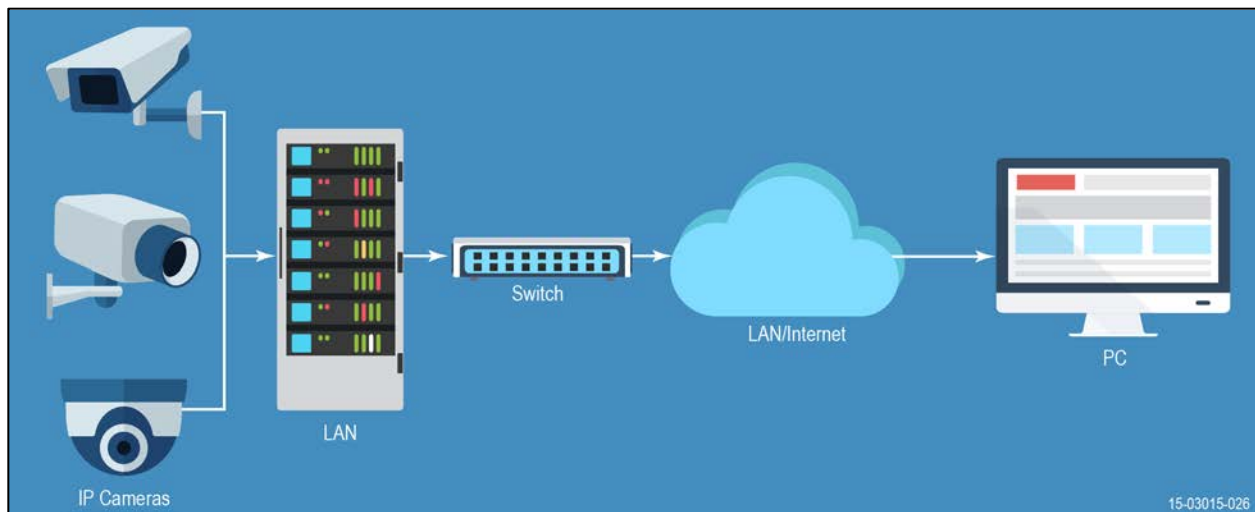


Figure 8-3 IP Camera and Network

A network-camera–based video system provides the following benefits (Reference 256):

- Ability to use high-resolution cameras
- Consistent image quality with no degradation of video signal between camera and display
- Ability to use power-over-Ethernet and wireless functionality
- Full access to functionalities such as pan, tilt, and zoom
- Ability to set camera settings and system adjustments over IP
- Full flexibility and scalability

8.3.3.1.6 Smart Cameras and Video Analytics

Manual analysis of video data is typically time consuming and requires dedicated staff. Identification of important events or suspects may be missed due to the monotony of manually analyzing large quantities of video data, most of which would likely contain nothing of interest. This has led to the development of video analytics, which is software that ingests and analyzes video data in an effort to provide information that may be relevant to the user. Using video analytics enables more rapid and

efficient analysis and reduces the number of staff-hours needed to monitor a large quantity of video data (Reference 18).

Video analytics is analytic software, not a type of camera. The software can be embedded in the camera or integrated into a video management system that can identify events and patterns of behavior through analysis of video streams. A smart camera is capable of extracting specific information from the captured images and video. Most smart IP cameras are capable of basic motion detection (by detecting changes in pixels), but cannot run analytic algorithms internally and thus require a separate processor for this analysis (e.g., facial recognition may be performed on a laptop or network computer). Some advanced IP cameras are equipped with embedded analytics (e.g., facial detection may be performed on a chip in the IP camera); however, a video management system is still needed for storing and reviewing video on a computer system. The analytic software monitors video streams in near-real time and generates alerts when certain predetermined activity is detected. Video analytics also assists with forensic analysis and promotes enhanced security coordination.

Video analytics systems can extract information of interest, such as license plate numbers or cars parked near a virtual fence, from the data and send alerts, if warranted. As a result, fewer school security staff are required to monitor these systems. In addition, a complete security system would allow integrating information from access control systems with a video analytics platform so that an intrusion alarm can trigger the system to record events near the area where an intrusion alarm has triggered, collect and analyze data, and send alerts along with related video feeds.

Features offered by video analytics are continually evolving and can be classified into three categories (basic, intermediate, and advanced) and include (but are not limited to):

- Basic features
 - **Object classification:** Identifying an object's presence and placing it into its proper class (e.g., person, vehicle)
 - **Object identification:** Specifying the object in the field of view (FOV) more uniquely than classification (e.g., car, truck, van)
 - **Motion detection:** Detecting the motion of any moving body in the FOV
 - **Tracking:** Detecting motion and following that motion through the FOV
 - **Alarm and alert generation:** Creating an alarm to notify the user of an item or action of interest in the FOV
 - **Tampering detection:** Detecting when an outside source is tampering with its normal operation (often paired with an alert generation)
 - **Zone intrusion:** Creating zones and areas within a field of regard (the range of potential fields of view for a movable camera) and then noting when an object passes into a zone
- Intermediate features
 - **License plate recognition:** Recognizing a vehicle license plate and then reading and storing that plate's information
 - **Facial detection:** Identifying the presence of human faces in an FOV
 - **Loitering:** Identifying individuals or objects that appear in an FOV and then stopping or "loitering" in that FOV for an amount of time
 - **Counting:** Identifying and then quantifying a known object or class of objects

- Advanced features
 - **Facial recognition:** Capturing unique features associated with specific human faces (for eventual comparison with other means of identification)
 - **Single-camera tracking:** Using a pan/tilt/zoom camera
 - **Multiple-camera tracking:** Transferring primary monitoring from one camera to another as a moving object travels between the fields of regard of cameras in a system.

For a more comprehensive list of features and other related information, refer to Reference 18.

8.3.3.2 Differentiators

As computing power continues to increase and the cost of video analytics decreases, schools still using analog systems should consider switching to IP-based digital systems to take advantage of the capabilities they provide. Video analytics systems do not function with analog images; therefore, integration with video analytics or other analytics would require analog-to-digital conversion.

8.3.3.3 Specifications and Features

The following general technical specifications should be taken into consideration when installing cameras and/or camera systems:

- **Camera type:** Table 8-2 identifies common camera types available for school applications. These categories are not all inclusive or individually unique (e.g., pan/tilt/zoom cameras may also be wireless).
- **Resolution:** Cameras are typically rated in megapixels (one million pixels). High-resolution (high-definition) cameras enable digital zoom features, which may prove useful in investigations.
- **Light requirements:** Some cameras can capture images in extreme low-light conditions. Others can capture infrared (IR) radiation, which is emitted by warm objects including people, allowing representation in complete darkness.
- **Range:** This is the maximum standoff distance of a camera, such that the analysis software can identify people, license plates, and other items of interest.
- **Pan/tilt/zoom:** This capability allows a single camera to view a wider area by moving up or down (tilt) and right or left (pan) and can change focus from near to far. They are good for outdoor applications.
- **Frame rate:** This refers to the number of individual frames that comprise each second of video. Frame rates in video typically range from 5 to 30 frames per second (FPS). Higher FPS results in smoother capture of movement.
- **Service life:** Duration of effective and cost efficient use of system.

Table 8-2 Common Camera Types

Camera Type	Description
Body-worn	Used with a video recording system, typically used by law enforcement to record their interactions with the public or to gather video evidence at crime scenes, but some schools have implemented their use. ⁴ Provides enhanced officer and citizen accountability.
Bullet	An indoor camera with a cylindrical shape. Mounted in a fixed location for monitoring a selected area.
Day and night	Adjusts according to varying light conditions. Mostly used for outdoor applications.
Dome	Dome-shaped camera. Cameras are visible, but are unobtrusive and their look-angle cannot be seen.
IR and night vision	Because they can detect lower frequencies than visible light, these cameras have the ability to capture images in pitch-black conditions. Can be valuable for exterior surveillance in low-light conditions.
Outdoor	Cameras with housing constructed to withstand heat, moisture, and other environmental factors.
Varifocal	Lens permits zooming in and out without compromising the focus of the image.
Wireless	Camera transmits its signal without a wireline connection to the destination.

8.3.3.4 Effectiveness

Before discussing the effectiveness of security video cameras, Wren and Spicer (Reference 389) provide general guidelines on properly deploying them:

- **Get the right people involved.** A cross-functional implementation team for video planning and deployment can decrease errors and ensure buy-in among critical system users. The team should include the principal, administrators, safety officers, Information Technology (IT) professionals, teachers, and athletic and transportation directors.
- **Capture the right video.** Prioritize coverage areas to provide the greatest possible breadth of information. Planning should consider a history of problems in the building and which areas are most frequently associated with activities such as fights, vandalism, drug use, and leaving school property without permission. Consider entry and exit doors, high-traffic public areas, loading and unloading areas for buses, corners and stairwells, restroom entrances and exits, and parking lots.
- **Leverage video with other systems.** IP video is unique in its ability to augment other systems. Schools should use video to capture and corroborate events and should position video cameras to help verify and increase the effectiveness of their other systems. Relating to access control, for example, administrators can use video to determine whether main entrances are being kept locked during in-class hours, thus forcing visitors to check in at the office. Video can also identify issues such as tailgating, propping doors open, and other activities that may render access control systems ineffective and suggest the need for related training.

The research team did not find a large quantity of published literature on the effectiveness of security cameras; findings in the articles discovered are mixed (Reference 2). Priks (Reference 281) found that

⁴ <https://www.takepart.com/article/2015/07/06/body-cameras-schools>

conspicuous security cameras can reduce unruly public behavior. Anecdotally, the research team was told by some school officials that video cameras on school buses drastically reduced fights and other misbehavior after their installation (Reference 163). Garcia, on the other hand, found that only 67% of the survey respondents believed cameras to be either effective or very effective (Reference 126). Consider the use of cameras in the following school areas:

- **Classrooms:** Place cameras out of reach of students. A wide-angle lens should allow most of the room to be visible from a ceiling-mounted camera. Observe the room entrances and exits. Although classrooms are public areas, privacy issues may be a concern, especially if teachers process student paperwork.
- **School office:** Of special concern in office environments is the presence of privacy-protected information, such as student behavioral and medical files, as well as privacy concerns for office staff and visitors.
- **Buses:** Cameras on school buses have been credited with reducing behavioral problems. Usually, video footage is downloaded from the bus at the end of each school day. Cameras should be placed as far out of reach of students as possible, or in areas where they may be observed by the driver.
- **Hallways, stairways, breezeways, covered walkways, and patios:** Cameras should first be installed in areas where lack of staff presence may be a security concern, such as stairwells or areas of low traffic. Security cameras are commonly placed in hallway intersections or at the ends of long hallways.
- **Common areas:** Place cameras in lobbies, gymnasiums, auditoriums, cafeterias, and libraries. Many incidents of school violence have occurred in these areas.
- **Transit areas:** Areas between school structures, especially temporary buildings (e.g., trailers, modular buildings, extensions) and the main school building are good candidate areas for cameras because of their lower visibility and lack of staff presence.
- **Bus loading and unloading areas:** Although these are often monitored by school staff, these staff may be overwhelmed by the large number of students transiting the area in a short time.
- **Sports stadium and athletic fields:** When Internet-linked cameras are available to law enforcement, this video surveillance may enhance the capabilities of security staff assigned to after-school sporting events.
- **Open spaces (e.g., quads):** Outdoor areas accessible only from the school building are not always monitored by staff, nor are they always easily visible from classrooms and offices.
- **Playgrounds:** Consider what areas may be obstructed by playground equipment when selecting camera locations.
- **Other entrances and exits:** Cameras should be placed to observe the doorways. In addition, the approach to these doorways should be covered from the outside, especially if other exterior cameras do not observe these areas.
- **Service areas:** Cameras may provide situational awareness in loading and storage areas, basements, furnace rooms, and utility rooms. These areas tend to be less trafficked and may be used as staging areas for acts of mass violence. These areas may also be more vulnerable for illicit entry into the building.
- **Secluded areas:** Some school sites include areas not visible from windows. Assaults and fights may occur more commonly in these areas because they are perceived to be less visible to staff.

The following guidelines should be considered when deploying cameras and camera systems in schools:

- Cameras installed in hallways should have sufficient resolution to identify persons throughout their field of regard. A camera installed in a parking lot should be capable of discerning license plate numbers, especially if analytics are capable of capturing license plate data. For example, to maintain a minimum of 40 pixels per foot (in the horizontal and vertical directions) specification using a 640×480 IP camera with a 3.0-mm lens,⁵ the horizontal FOV would be 34 feet wide at a distance of 25 feet from the camera. To maintain facial recognition, the subject would have to be 7 feet or less from the camera; at 25 feet there are only 17 pixels per foot, which is not enough for facial or license plate recognition.⁶
- Consider placing cameras in areas of greatest utility (i.e., where visibility is most often required), such as the main entrance after the doors are locked, transit areas between the main building and extension buildings, and other areas not readily visible to school staff.
- Cameras installed at a main entrance should function in a variety of lighting and environmental conditions. Cameras should have sufficient resolution to assess safety risks of allowing entry to school.
- Cameras placed outdoors on school grounds should be rated for exterior use. This is an appropriate application for pan/tilt/zoom cameras because of the long sight lines and wide areas that may be observed.
- Integration with alarms and sensors, fire alarms, access control technology, and communication systems can enhance the effectiveness of surveillance equipment. For example, a burglar alarm may automatically trigger cameras in the area, allowing security staff or law enforcement to characterize the threat. Cameras synchronized with other sensors may also be used to quickly validate a fire alarm or localize an active shooter.
- Interoperability with legacy systems should be considered. Purchasers should research any camera system under consideration for compatibility issues with existing systems, especially if analog cameras are already in place. If a complete system replacement is not affordable, operating two parallel camera systems may be necessary until legacy analog cameras can be replaced with digital technology.
- Security staff should be able to copy footage of interest to a separate storage device (e.g., a server, hard drive, or other storage media) to preserve evidence or conduct further analysis. Provide adequate data storage capacity. Often, video data are kept for a predetermined length of time such as 7 days, 30 days, or 180 days before deletion.

8.3.3.5 Policy Impacts

Implementation of this technology requires a well-defined, known, and practiced policy regarding the intended use, monitoring, access, and storage of video content. In addition to the previous recommendations, Wren notes that “schools should anticipate negative reaction to the use of video and construct an official policy outlining its use. The policy should communicate why administrators chose to use surveillance technology and list general guidelines and restrictions of surveillance video. Developing and proactively communicating a plan can address concerns, garner support from the outset, and avoid being put on the defensive.”⁷

⁵ <http://www.aronsonsecurity.com/blog/bid/45150/Video-Surveillance-Camera-Resolution-How-Much-is-Too-Much>

⁶ http://www.toshibasecurity.com/resources/white-papers/Toshiba_Design_an_IPSystem_WhitePaper.pdf

⁷ http://www.toshibasecurity.com/resources/white-papers/Toshiba_Design_an_IPSystem_WhitePaper.pdf

Wren additionally notes that if possible “...law enforcement and firefighters should have a link via a web browser to provide access to live video from cameras on campus. The school may choose to offer full access to camera views any time, any place, or to offer video access only in case of an emergency. Either choice involves working through the school’s IT administrator and security personnel (Reference 389).

8.3.4 CONCERNS ABOUT THE TECHNOLOGY

8.3.4.1 General Discussion (What It Does Not Do)

Cameras may be useful tools in deterring, identifying, and investigating crimes and other unwanted or unauthorized behavior in schools, but they do not prevent such actions, especially when unmonitored. Staff and students should be aware of their presence, but should not rely on them as an immediate protective measure. To facilitate action in the event of a crime or other emergency, other systems (e.g., communications devices, call boxes, alarm triggers) can be integrated or available nearby.

8.3.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

Vulnerabilities and concerns about the camera technology include the following:

- Culprits may know where the cameras are located and be able to cover their faces or take other steps to mask their identities.
- People may relocate prohibited behaviors to areas without camera surveillance. School officials may consider frequently relocating wireless portable cameras to counter these adaptive behaviors.
- Cameras in schools are prime targets for student vandalism. Exposed wires may easily be cut and lenses obscured, covered, or blurred. Protective coverings may mitigate some of these vulnerabilities.

A study by Kaspersky Lab⁸ found that video surveillance networks can be easily hacked. An intruder may connect to a single node in the network and manipulate data. By recreating the network and software, Kaspersky Lab researchers were able to intercept video feeds from any node and replace them with fake video feeds.

8.3.4.3 Possibilities for Misuse

Cameras could potentially be misused by those who have the authority to access or direct their coverage area, use, and other factors, or by those who access the systems through unauthorized hacking. Strict access and use policies may deter this behavior. Additionally, access logs and stored video should be periodically monitored for evidence of camera misuse.

8.3.4.4 Liability and Safety Concerns

The research team found no significant safety concerns associated with the use of cameras.

8.3.4.5 Privacy Concerns

Federal, state, district, and school policies, laws, and regulations concerning civil liberties and privacy rights may prohibit or restrict the use of video security in some cases (e.g., use of cameras in areas

⁸ <http://www.kaspersky.com/about/news/press/2015/Video-Surveillance-Systems-under-attack-how-hackers-could-modify-video-feeds-in-misconfigured-city-CCTV-systems>

where there is a reasonable expectation of privacy). For cameras equipped with microphones, some states do not allow audio recording of any conversation without consent from all parties. Prior to deploying a camera or camera system (or cameras with upgraded or enhanced capabilities), relevant laws should be reviewed. Caution should be taken to determine what images and videos are subject to Freedom of Information Act (FOIA) requests for disclosure to the public.

8.3.4.6 Accommodations for Persons with Disabilities

In general, no special accommodation is needed for disabled persons being monitored by camera systems. If the system is operated or monitored by persons with disabilities, some special accommodations may be necessary and should be considered according to the vendor and specific technology selected.

8.3.4.7 Policy Concerns

Public perception may impact the use of camera systems in schools. Placing cameras in any part of the school building may result in controversy over privacy concerns, particularly when policies and information about the cameras are not openly shared with all stakeholders (i.e., students, teachers and other school staff, and the community). Additionally, policies on the length of time recorded video feeds are to be stored (e.g., 30 days from the day of recording) should be strictly followed. Stakeholders should be aware of these policies and any exceptions (e.g., recorded video being used as evidence in court will be stored as long as the court, or some other jurisdictional entity, dictates). And again, decision-makers should fully understand whether captured images are subject to FOIA requests because these requests represent a concern for student and staff privacy as well as unplanned costs to furnish the requested files.

8.3.5 COST CONSIDERATIONS

Traditionally, IP cameras have been more expensive than other digital cameras; however, as the technology improves and the market transitions more to video, this may no longer be the case. The total cost of purchasing and maintaining IP cameras is becoming less expensive than that of analog cameras, according to some studies (Reference 189).

Security cameras and systems are expensive to install and maintain. Additional equipment such as recording media (tapes, compact disks, and DVDs) and systems such as video analytics will increase the total cost of technology. Maintenance and operational support may demand future funding. Selecting the right camera and supporting devices requires deep technical knowledge; a person with technical expertise in security cameras, analytics, and accessories should be consulted prior to procurement decisions.

There are numerous variables, such as the security needs of a school; the number, types, and price of security cameras suitable for the school; type of video processing; and supplementary devices such as DVR or network video recorder (NVR). Given such variability, it is difficult to provide even a range of costs in general terms. Nilsson (Reference 256) reports that a study conducted in 2007 by an independent researcher compared the total costs of ownership associated with two surveillance systems: an analog surveillance system and an IP-based video surveillance system.

Given the caveats previously noted, the cost factors in Table 8-3 should be considered general and variable according to specific vendors and other factors.

Table 8-3 Camera Cost Considerations

Cost Factors	Cost Description
Acquisition	For a small school with 32 cameras (with no video analytics), cost may be approximately \$75,000 to \$80,000. For the same school with video analytics, the price likely doubles. NVRs and other devices are normally bundled in the price.
Installation	In some cases, this is part of the acquisition cost. In other cases, this is a one-time cost and may be higher for wired systems than for wireless systems.
Operation and labor	For simple systems, casual monitoring is needed. Dedicated staff may not be needed in most schools. In the event of an FOIA request, substantial labor hours and costs may be incurred to identify and redact the requested imagery files.
User training	User training (done either locally or remotely) should be provided by the system or camera vendor and is often included in the purchase and/or installation price. Ongoing training may require an additional charge.
Maintenance	Maintenance functions are highly variable and dependent on the type and number of systems. Hardware (e.g., camera bodies, wiring) and software (e.g., monitoring systems, video analytics capabilities) will need to be maintained regularly.
Consumables	Consumables such as replaceable dome covers, light bulbs, etc., may be necessary dependent on the camera type.
Energy and energy dependency	Cameras and data networks require power, which may be lost in a natural disaster. A plan for backup power (e.g., generator) should be established.
Software licenses	Special monitoring software may be available from camera and video analytics vendors. Often, software licenses need to be periodically updated after initial purchase to maintain monitoring capability.
System integration	Camera systems can be integrated with other security measures (e.g., alarms, speakers). Cost of this integration can vary highly.

8.3.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

Many schools are likely to have legacy (often analog) camera systems in place. Replacement of these existing systems can be done incrementally or all at once as newer digital units are integrated. The more advanced wireless and IP cameras have higher potential for integration with other security systems. Specifically, as mentioned in this report, video analytics capabilities in these systems are becoming more sophisticated and reliable, and should be reconsidered on a regular basis.

8.3.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 8-4 presents examples of known vendors of video products; however, it is not comprehensive and other vendors may exist. The list is current as of 2 February 2016.

Table 8-4 Surveillance Camera Vendors

Vendor	Website	Comments
Bosch	//us.boschsecurity.com/us_product/products/video/analogcameras/analogcameras_14	Analog
Hyundaitel	http://www.hyundaitel.com	Analog
Pelco	https://www.pelco.com/video-surveillance-camera-security-systems/analog	Analog
Rugged CAMS	www.rugged-cctv.com/infrared-choices.shtml	Analog
SAMSUNG	https://www.samsung-security.com/products/security-cameras/analog-cameras.aspx	Analog
Truetelecom	http://www.truetelecom.org/surveillancecctv.html	Analog
Axis	www.axis.com/node/37607	IP
Canon	www.usa.canon.com	IP
HIKVISION	www.hikvision.com	IP
Samsung	https://www.samsungsv.com/	IP
Vivotek	www.vivotek.com/	IP
Y-Cam	https://www.y-cam.com	IP
Zavio	www.zavio.com	IP
3VR	http://www.afnsolutions.com/3vr	Video analytics
3Xlogic	https://www.3xlogic.com/3xproducts/vigil-systems	Video analytics
IBM	www.ibm.com/IntelligenceAnalysis	Video analytics
IPVM	http://ipvm.com/products/VideoAnalytics	Video analytics
Mango	https://www.3xlogic.com/3xproducts/vigil-systems	Video analytics

8.4 GUNSHOT LOCATION SYSTEMS

8.4.1 INTRODUCTION

Gunshot location systems detect a gunshot, identify the gunshot’s location, automatically generate an alert, and send the alert to first responders and others on a predetermined notification list. Vendors use software that interprets the input from a system of acoustic sensors and/or IR cameras to detect the sound of a gunshot and the associated visible “muzzle flash” of high-temperature, high-pressure gases emitted by the firearm.

Before examining gunshot detection technology, it is instructive to review the historical data on active shootings in the United States. According to an FBI study (Reference 110), about 17% (27) of active shooter incidents took place in schools (Pre-K to 12) in the United States from 2000 to 2013.

In addition, the FBI study states that:

- In 64 incidents (not limited to educational environments), where the duration of the incident could be ascertained, 36% ended in 2 minutes or less and 69% ended in 5 minutes or less.

- When shootings impacted a school, the incidents occurred in classrooms, hallways, the cafeteria, administrative offices, and school board meeting rooms. Incidents also began outside school buildings and in vehicles on school property.

Vendors and proponents of gunshot detection technology frequently note that the average duration of a shooting event is 12.5 minutes, and the average response time of local law enforcement is 18 minutes (Reference 106). Gunshot location technology is one means by which law enforcement could be notified and respond more quickly, thereby potentially saving lives.

There are two types of latency associated with this technology:

- The time it takes from the gunshot being “heard” or “seen” by the sensor and the time it takes to generate an alert
- The time from alert generation to delivery to the appropriate notification list

8.4.2 HOW THE TECHNOLOGY IS USED

Gunshot detection is a technology category with few systems currently in place. The technology can save lives in an active shooting event by providing early warning that an incident is occurring. By detecting and alerting almost instantaneously following a gunshot, this technology allows students, staff, and other building occupants to immediately take protective actions. In addition, first responders can be concurrently alerted for quick dispatch to the shooting location and provided information on a map that shows the initial and subsequent gunshot locations.

Although independent data on latency, false positives, and false negatives are not available, alerts can theoretically be generated within seconds of gunshot detection.

8.4.3 WHAT MAKES THE TECHNOLOGY GOOD

8.4.3.1 How the Technology Works

The system consists of a network of deployed optical (IR) and/or acoustic (microphone) sensors, which can be deployed indoors or outdoors with the intent of creating a web of overlapping detectors. The sensors detect a loud sound’s characteristics and consult a library of sounds to determine whether a shot has been fired. This is done through communication with an associated computer server or, in some cases, through live agents who confirm the analysis. The vendor’s software can then triangulate the location of the gunshot based on differences in detection times among sensors and display the location on a map.

Depending on the vendor product, a nearby microphone may be turned on for a short time period to capture additional data. Some vendor products deploy gunshot sensors on security cameras so that cameras can be triggered to zoom in on the direction where the gunshot was detected and send a video signal for recording.

Additionally, the associated computer server system can be programmed to follow a list of commands once the gunshot is confirmed. This could include (order may differ) any or all of the following:

- Send contextualized alert including audio and video files, if supported by the vendor, to 911 operators and other first responders.
- Send notification to teachers and administrators.

- Send landline phone calls with automated prerecorded computerized messages to a predetermined list of individuals.
- Initiate lockdown procedures.

Figure 8-4 presents a notional gunshot detection system architecture. Analytical components of these systems (i.e., algorithms for analyzing sound and light) are sometimes embedded in the sensors themselves or may be on a server. Each sensor can send its location to a server. The server contains the software integration such as situational awareness applications, notification list of people to be contacted, sequence of alerts, etc. The server sends the alerts to cellphones, sends emails, etc. In many installations, the server is a shared resource among many buildings.

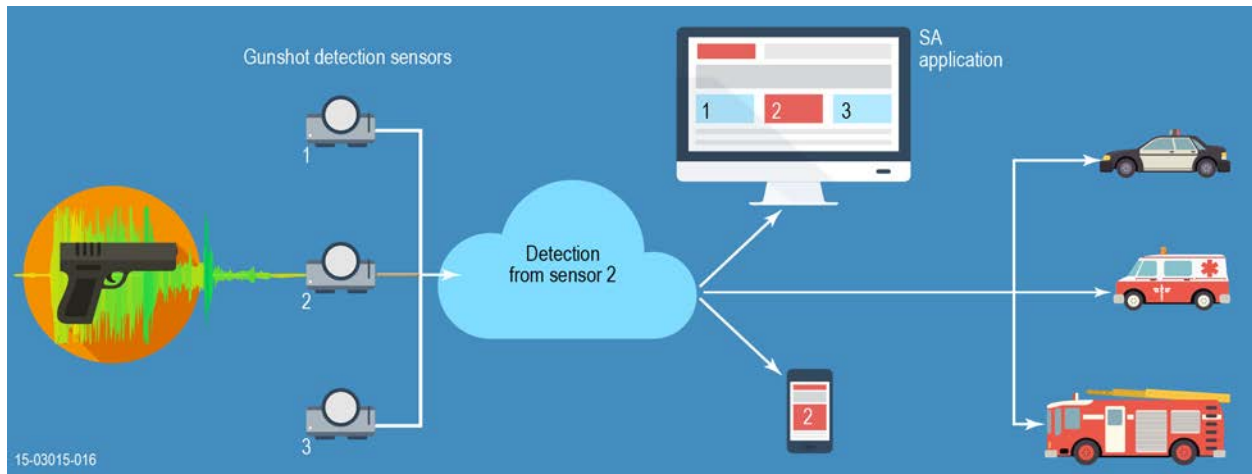


Figure 8-4 Notional Gunshot Detection System Architecture

8.4.3.1.1 Differentiators

Vendor products vary considerably. Some can be used only indoors, whereas others can be used outdoors as well. In addition, different systems analyze alerts in different ways. Some are fully automated, where sophisticated software analyzes the audio file, whereas others require that a person analyze the audio file to confirm the alert is a gunshot.

8.4.3.1.2 Specifications and Features

In addition to the features previously discussed (e.g., notification and mapping options), specifications for specific sensors and sensor systems vary by vendor. The following technical parameter values are estimates:

- Size of sensor plates: 4.6×4.6×1 inches
- Weight: one-half pound (sensor module)
- Power: Standard power-over-Ethernet or 5 to 24 volts direct current (VDC)
- Sensor coverage: 70 to 100 feet
- Mounting configurations: flush (e.g., wallboard or ceiling tile) or box (e.g., with concrete or brick structures)
- Network interface (e.g., 802.3 10/100M compliant, CAT 5E cable)
- Sensor life: approximately 10 years

8.4.3.1.3 *Effectiveness*

The research team did not find much published literature on the effectiveness of gunshot location systems. Although such systems may be currently in use in government buildings or other critical infrastructure, the following guidelines should be considered before deploying these systems in a school environment:

- To remove critical minutes from the response time, integrate a system to the extent possible with local first responders, and test the system via a number of realistic emergency response scenarios.
- Provide and make available current maps with incident and location details. Maps and blueprints of schools and grounds should be preloaded into the vendor's software (and available to first responders) so that an accurate location of gunshots and deployment of responders is possible.
- Ensure the vendor product offers a chronological sequence of events for all recorded events and alarms. The system should also capture an accurate location of the gunshot, the number of shots, and the time of the shot(s).
- Endeavor to integrate this system with other sensors and security technology (e.g., access control systems and security cameras) whenever possible. Detected gunshots could cue other sensors, especially cameras and microphones, and alert systems to expedite first responder and staff awareness and enable mitigating actions.
- Conduct planned school security drills to validate the efficacy of this system and assess its utility in directing emergency responses.

8.4.3.1.4 *Policy Impacts*

Implementation of this technology requires a well-defined, known, and practiced policy regarding school emergency response actions including directions for all stakeholders (e.g., staff, students, local first responders) in the event of the system triggering an alarm. In addition, because of the associated potential need to block or deny access to entrances and exits or other school areas during a response, consider any Federal, state, and/or local fire laws pertaining to building access and safety. Ensure closed doors continue to be accessible as a means of egress whenever possible.

8.4.4 *CONCERNS ABOUT THE TECHNOLOGY*

8.4.4.1 *General Discussion (What It Does Not Do)*

Although the technology can be used to detect and locate gunshots, it cannot prevent a shooter from engaging in this activity nor can it actively track the shooter in real time other than by means of gunshot sounds. Merely recognizing that a gun has been fired has no effect on school safety, unless the that knowledge is used to immediately initiate safety procedures. This technology is best suited for decreasing incident alert and response times. Integration with other security technologies (e.g., lockdown systems, cameras) may increase the usefulness of the technology.

8.4.4.2 *Vulnerabilities and Possibilities to Circumvent or Defeat*

A major vulnerability of the gunshot location system is its reliance on power and the Internet. If either of these items is unavailable, the detection system will be incapacitated. Lack of redundant equipment such as gateway servers and switches in the system may also be a concern.

Although a shooting incident could be initiated either indoors or outdoors, vendor offerings intended for both venues are limited.

Another area of vulnerability is potential false alarms that could be generated due to sounds similar to gunshots such as fireworks, a car backfiring, or special tools used by nearby construction workers.

Additionally, tests should be conducted to ensure the system cannot be defeated or circumvented by the use of small-caliber weapons or quieter subsonic guns that absorb light and sound.

8.4.4.3 Possibilities for Misuse

Students who are aware of the system's intended use could try to spoof the system by using prerecorded sounds or some other means or mimicking the sound of gunfire, either as a prank or to draw a response to the wrong location.

8.4.4.4 Liability and Safety Concerns

A major advantage of gunshot location systems is their ability to quickly (and often automatically) notify first responders in the event of active gunfire on school grounds. Because these systems may trigger police response and expenditure of significant resources, careful coordination among local law enforcement agencies should be conducted at all stages of system installation and use. This coordination should include a review of applicable Federal, state, and local laws.

8.4.4.5 Privacy Concerns

Gunshot location systems do not collect personal information and therefore there are no current privacy concerns associated with these systems.

8.4.4.6 Accommodations Needed for Persons with Disabilities

Gunshot location systems do not have a direct impact on persons with disabilities. Should these location systems be integrated with other security technologies (e.g., lockdown systems), appropriate considerations for those systems should be made.

8.4.4.7 Policy Concerns

Because gunshot location systems are not currently widely used in schools, policies regarding their use and the associated response should be clearly communicated with all stakeholders (including the local community).

8.4.5 COST CONSIDERATIONS

The cost of gunshot location systems is a function of many variables, such as the number of sensors, type of sensors, size of school, floor plans, layout of network architecture, and many more. Table 8-5 provides some general gunshot location system cost considerations.

Table 8-5 Gunshot Location System Cost Considerations

Cost Factors	Cost Description
Acquisition	The cost of these systems vary; they often include acquisition of sensors, switches, software and server, etc. As an example, one vendor estimated \$100,000 for a “turnkey solution” (assuming sensor deployments at corridors, cafeteria, office, gym, major entry and exit points, and an average price of \$1000 per sensor). A second vendor estimated \$30,000 for a system with 13 sensors.
Installation	Installation costs will vary depending on type and complexity of sensors, sensor locations, etc. Installation costs may include mounting the sensors, modifying infrastructure to accommodate cables, etc.
Operation and labor	Operation costs are minimal because these systems do not need to be monitored and are intended to generate alerts automatically.
User training	Initial training should be provided by the vendor and should include all system stakeholders. Additionally, costs may be associated with periodic drills and other training, especially those that are coordinated with local law enforcement entities.
Maintenance	System maintenance may include occasional sensor checks and replacement, software updates, etc.
Consumables	None known.
Energy and energy dependency	These systems are dependent on power and a functioning network. Automated alert systems rely on a functioning Internet and telephone network outside the school.
Software licenses	Software licenses are often included in the initial purchase price of gunshot location systems, but will likely need to be periodically updated or repurchased.
System integration	Gunshot location systems have the potential for integration with other systems (including security cameras). The cost associated with this integration will be highly dependent on the type and extent of integration necessary.

8.4.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

Although there is no immediately obvious emerging technology in this category, new technology development may not always originate from commercial vendors. Cities, dispatch centers, and school districts may combine their efforts to develop new, similar applications. For example, the city of Ammon, Idaho, developed a School Emergency Screencast application that integrates with a school’s existing camera system, the city’s fiber-optic network, high-speed Internet, and gunshot sensor technology.⁹ This integrated system is designed to provide a live feed to emergency dispatch if an active shooter incident happens.

8.4.7 VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 8-6 provides examples of known vendors of gunshot location system products; it is not comprehensive and other vendors may exist. The list is current as of 3 February 2016.

⁹ Bonneville County and Bonneville Joint School District 93 in Idaho Falls, Idaho

Table 8-6 Gunshot Location System Vendors

Vendor	Website
Battelle	Battle.org/siteguard-ASR
Guardian Indoor Gunshot Detection	www.shooterdetectionsystems.com
SENTRI (Sensor Enabled Neural Threat Recognition and Identification)	www.safetynamics.net
SST Inc. (ShotSpotter Flex, ShotSpotter SiteSecure, Secure Campus)	www.shotspotter.com
RedAlertt, LLC	www.shotalarm.com

8.5 LOCATION TRACKING SYSTEMS

8.5.1 INTRODUCTION

A 2012 school bus safety transportation report by Cook and Shinkle (Reference 74) noted that “[m]ore than 450,000 yellow school buses transport 25 million children between school and home each day. That number represents about 55% of the K-12 population. School buses travel approximately 4.3 billion miles annually, keeping about 17.3 million cars off the roads surrounding schools each morning.” The vast number of buses and students riding them presents a daunting task in keeping them safe during transport. Knowing where the buses and students are is one way of doing so.

Some schools use radio frequency (RFID) or GPS technology to track the movement of students and buses. These two technologies are not mutually exclusive and can be combined (e.g., while tracking students in a school bus on a field trip).

With an RFID-based system, a student carries an identification card or a bracelet with an embedded RFID chip. Each chip is encoded to uniquely represent a particular student. Location is recorded when the RFID card or bracelet is presented to a fixed RFID reader adjacent to a door or when it comes in close proximity to an external RFID antenna reader. With a GPS-based system, the student or bus carries a GPS-enabled device. The device computes its position (and by extension the student, staff member, vehicle, visitor, or special asset carrying it) by processing satellite signals. Both applications report their location to a central monitoring system, and some permit tracking entities as moving points on a map.

This type of enhanced situational awareness reduces the likelihood of leaving students on an empty school bus at the end of a route, in an empty building at the end of a school day, or at a field trip site. In the event of a school emergency, these Internet-accessible data records may be also used for accountability or forensics.

8.5.2 HOW IS THE TECHNOLOGY USED

Location tracking and monitoring systems enhance safety by providing situational awareness to concerned parties. This technology is useful if the information can be accessed and understood in a timely manner, allowing staff to identify which students were present in a given room at a certain time, or to follow the progress of a student through a school day. By combining RFID and GPS technology, schools can accurately determine bus ridership count, identify missing students, or monitor students during field trips and other outings.

Schools install GPSs in school buses to track their location and to create more efficient routing. Issues that arise regularly include children missing their school bus in the afternoon, missing their stop, or getting off at the wrong location. This can lead to fears of serious criminal incidents, such as child molestation, kidnapping, etc. Location and monitoring systems can be effective in preventing or at least notifying school authorities when students are not where they belong. School staff and administrators are not the only people who need to know that a student has or has not boarded his/her bus at the stop or school or exited the bus at school or home. These devices can also provide convenient notifications to parents, which will show them their child's real-time location.¹⁰

In another system, students carry a passive RFID card that they scan as they enter or exit the bus. The time, date, and location of each scan is logged and transmitted to a secure database for immediate access.¹¹ The devices can also monitor the pupils' movements on campus and track them as they come and go from school.

The Spring Independent School District in Houston announced results of its program in 2010. "RFID readers situated throughout each campus are used to identify where students are located in the building, which can be used to verify the student's attendance for ADA funding and course credit purposes."¹²

8.5.3 WHAT MAKES THE TECHNOLOGY GOOD

8.5.3.1 How the Technology Works

RFID-based and GPS-based tracking differ by the technology they use as well as the frequency with which the track is updated. RFID-based tracking takes place each time an RFID chip comes in close contact with a reader, whereas GPS-based tracking is continuous (as long as satellite signals are available), and location data can be obtained at recurring preselected time intervals. Each is described in greater detail next.

8.5.3.1.1 RFID-based Tracking Systems

Depending on the needs of the school, tracking arrangements may be long term, with tracking devices included in each student's school identification card, or short term, with devices such as RFID wristbands given temporarily to students for field trips or other special events. These devices may also be attached to students who have cognitive or behavioral disabilities, allowing staff to maintain a heightened awareness of their location, or may also be used in conjunction with geofences, a feature in a software program that uses the GPS or RFID to define geographical boundaries where the monitoring system is programmed to generate an alert if a virtual fence line is crossed. Lastly, this type of system may be used to track school staff and enable security personnel to coordinate staff movement efficiently during a crisis.

An individual's presence is recorded when the RFID chip on an identification card or wristband is read by an RFID antenna reader. Using radio waves within its wireless range, the reader communicates with the RFID chips and collects information about the individual, as illustrated in Figure 8-5. Students' RFID cards or wristbands have a passive RFID chip imbedded. As they swipe near an RFID reader, the reader sends

¹⁰ <http://www.trackschoolbus.com/school-transportation-services/>, accessed 12 February 2016.

¹¹ <http://zonarsystems.com/solutions/z-pass-student-tracking/>, accessed 12 February 2016.

¹² <http://www.wired.com/2012/09/rfid-chip-student-monitoring/>, accessed 12 February 2016.

out a signal to the chip and the chip returns the proper identification to the reader. If this identification matches an identification in the RFID database, the student is granted access to the secured space.



Figure 8-5 RFID-based Tracking Inside a School

The collected data are transferred to a central database for storage. This database contains student registration data including time stamps. Students may also be required to “swipe” or “scan” out of facilities or classrooms, with the system then registering the student’s departure. RFID-based tracking can also be performed while registering students boarding or disembarking from their school buses. The data can be forwarded to school administrators’ or parents’ smartphones.

8.5.3.1.2 GPS-based Tracking Systems

GPS is a worldwide radio-navigation system formed from the constellation of more than 30 satellites and their ground stations. GPS is mainly funded and controlled by the U.S. Department of Defense. The system was initially designed for the operation of U.S. military, but today there are also many civil users of GPS around world. The civil users are permitted to use the Standard Positioning Service without any kind of fee or restrictions.

For a GPS tracking system, the student is provided a tracking device that reports its location through a wireless network to a tracking system on a central server. The tracking device uses geolocation data to determine its own location. No interaction with any point sensors (such as antenna readers) is required—the system receives data from the device and updates location information at predetermined intervals, often continuously. Location data may also be displayed in real time on a computer map.

For a GPS bus location system, the vendor-provided GPS unit or platform in the bus receives GPS data and computes the location of the bus. The bus then transmits its location data, typically over a wireless cellular connection, to a secure server. The Internet transfers information to and from the secure server to customer workstations, computers, and mobile devices such as iPads and cellphones. Schools log in to the websites, identify the school bus of interest, view the bus status and its location on a map, and take

any actions, if needed, as illustrated in Figure 8-6. Administrators not only receive information, but can also interact with and control the fleet by sending messages, directions, and geofencing data to the buses. Some schools may allow parents to register for the service and access limited GPS information about their child’s bus through school webpages.

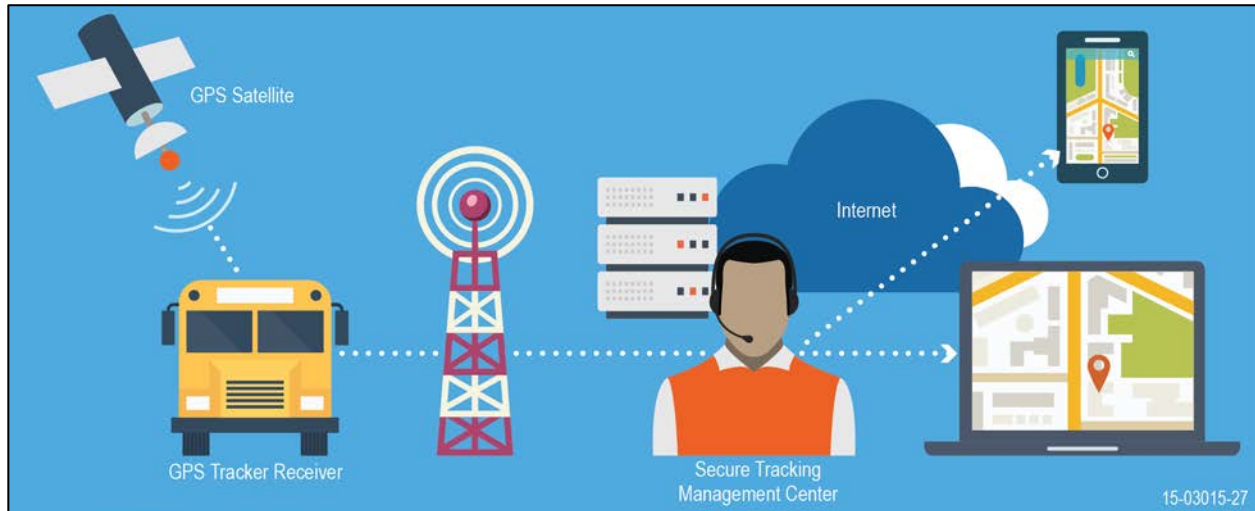


Figure 8-6 Notional GPS Bus Tracking System

8.5.3.2 Differentiators

There are several advantages to using location-tracking systems (RFID or GPS):

- Tracks students and staff on campus, buses, or field trips
- Provides proper access to secured areas
- Provides alerts when buses or students arrive and leave the geofences
- Potentially reduces the bus fleet cost by providing information to optimize routes
- Suggests alternative routes to bus drivers during road congestion or construction times

8.5.3.3 Specifications and Features

Tracking technology can be evaluated with respect to the following performance parameters:

- **Accuracy of location information:** Item of interest location error, in meters
- **Update rate of location information:** The delay between movement of tracked entities and the update of information in situational awareness software
- **Update rate of alert information:** The delay between detection of an alert event and the update of this alert in situational awareness software
- **Web-access latency:** What delay does the user endure between querying the system for information and receiving the information?
- **Reliability:** Can the system perform its required functions under stated conditions?
- **Availability:** What percent of the time can vehicles be tracked vs. what percent of the time the school bus location is unavailable?
- **Coverage of operating area:** What percent of a school bus’s route is in “uncovered” areas, i.e., where it drops out of cell coverage and does not transmit its location? What percent of the

route is in areas, like urban or geologic canyons or under heavy tree cover, where GPS signals are unavailable?

8.5.3.4 Effectiveness

The research team did not identify substantive published literature on the effectiveness of mitigating acts of criminal violence through the use of location systems used in schools or on buses. As more schools adopt this technology, more statistics should become available.

8.5.3.5 Policy Impacts

Implementation of this technology requires a well-defined, known, and practiced policy regarding its use. Policies should include descriptions of use of various components of the technology such as the RFID tags, scanners, and racking software in addition to any potential risks (e.g., gaining unauthorized access to the student tracking software), and the security steps taken to minimize the risks. The selected student tracking system should be thoroughly evaluated with respect to safety and privacy impacts.

Schools should have comprehensive documents and policies about the deployment of these systems. If parents or other stakeholders will have access to any data, they need to be informed as to what data are available and for what purpose. All stakeholders should be trained in accessing and using school websites or other interfaces for obtaining any available location data. Schools should consider:

- Encrypting and/or password protecting access to location information
- Providing limited access to authorized users on a need-to-know basis
- Protecting the school district's own private database

8.5.4 CONCERNS ABOUT THE TECHNOLOGY

8.5.4.1 General Discussion (What It Does Not Do)

These location systems are useful for tracking individuals or resources. These systems cannot be definitively relied on to identify the actual individual or resource with which the system is associated because misuses or mistakes may cause one student to carry another student's identification card. Additionally, these are location systems only—they do not provide physical protection from any specific event or threat. They may have significant awareness or forensics utility, but should not be relied on for real-time emergency decisions unless the system deployed is stringently tested in such conditions.

8.5.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

8.5.4.2.1 RFID-based Tracking Systems

Components of the tracking system such as the RFID chips and the antenna receivers can fail on their own or can be compromised by vandals. When there is loss of signal (tunnels) or dead spots in cell networks (rural areas), many tracking systems lose their capability to collect and transfer data.

Care must be taken that student presence is registered appropriately by the system. Cards often do not register on the first attempt. An audible and/or visual signal indicating a successful entry should be required for each student's interaction with the tracking system. Failure to follow this protocol will result in false entries that reduce confidence in the system, particularly if alerts are generated when a student is incorrectly assumed to be absent.

Procedures need to be established for when a student's identification card fails to register in a reader so as to maintain situational awareness of the student's location. Note, however, that possession of a card does not ascertain a student's identity.

Identification cards can be easily lost. Practices should be implemented that allow for a quick adjustment when a student loses or forgets an identification card. False alerts, particularly for missing students, will erode user confidence in the system. This will cause unnecessary security intervention or, worse, encourage operators to ignore system alarms if false alerts become commonplace. Some precautions include the following:

- RFID cards should contain only limited essential data (no detailed data on students).
- RFID tags have been shown to be vulnerable to devices programmed to read them in public settings. Data contained in RFID tags should be coded to limit its detriment if compromised.
- Security staff should consider using encrypted and password-protected tracking software.
- Provide limited access to systems on a need-to-know basis.
- Protect the school district's own private database.

Lack of encryption makes it easier to clone a card, allowing someone to impersonate a fellow student or to create a substitute card to play hooky, and makes the cards readable by anyone who wanted to install his/her own RFID reader.¹³

8.5.4.2.2 *GPS-based Tracking Systems*

Operators that monitor location-tracking systems should be familiar with the layout of the school and all areas displayed on the tracking map. They should also be aware that a loss of GPS signal could reduce the effectiveness of GPS tracking systems. If available, geofences may be used to ensure tracked students remain in assigned areas. Care should be taken that students do not discard their tracking devices to avoid detection. Security staff should not become overly reliant on location tracking systems; an intruder will not be wearing a location device, and a student will likely remove it before committing a violent act.

For buses specifically, vulnerabilities related to the technology include loss of signal when buses are in tunnels or parking garages (although some vendors claim their products work in these locations as well).

8.5.4.3 *Possibilities for Misuse*

Students or bus drivers can be careless when using these devices. For example, drivers may allow students who have not completed their registration process to board, or students may fail to swipe their cards, which would result in lack of data. Additionally, ID cards or other RFID devices can be used by the wrong person to hide the actual location of the intended owner. For example, a student could ask another student to swipe his/her badge to cover an absence, or an abductor could slip a child's badge into the belongings of another student about to board a school bus to generate false information about the child's whereabouts. And because these systems offer the ability to track the movements of individuals, it is possible for someone with access to the tracking information to use it to stalk someone.

¹³ <http://www.wired.com/2012/09/rfid-chip-student-monitoring/>, accessed 12 February 2016.

8.5.4.4 Liability and Safety Considerations

GPS tracking, data security, privacy rights, and potential legal issues are key concerns that the school district should address prior to implementing these technologies. Districts must investigate the local and state statutes on privacy to ensure any information collected by the system complies with local and state statutes on privacy to avoid any civil complaints.

8.5.4.5 Privacy Concerns

On the non-technical side, a significant challenge facing school districts planning to use RFID or GPS technologies is related to public perception and the concern over violation of privacy rights.

8.5.4.6 Accommodations Needed for Persons with Disabilities

In general, location-tracking systems do not require accommodations for persons with disabilities. However, the system should be evaluated for its impact on such persons. It is important to ensure identification badges and card readers are accessible to all users and do not interfere with existing or planned accessibility features.

8.5.4.7 Policy Concerns

To minimize potential controversy or other policy complications when deploying location systems, school administrators should educate all the stakeholders impacted by the technology (e.g., staff, students, parents, bus drivers) on the rationale behind its use.

8.5.5 COST CONSIDERATIONS

The purchase prices of location tracking systems vary. Vendors often offer options to purchase hardware upfront or select a service bundle that includes hardware, software, installation, and ongoing support with monthly fees. Some cost considerations for these systems are described in Table 8-7.

Table 8-7 Location Tracking System Cost Considerations

Cost Factor	Cost Description
Acquisition (GPS tracker or locator)	GPS systems for school buses can be purchased for approximately \$1950 per bus with additional administrative hardware for \$32,000.
Installation	Installation costs will vary based on the number and types of sensors, cards, and other infrastructure including monitoring hardware and software.
Operation and labor	Monitoring the GPS devices will require some labor, although this may be relegated to data retrieval for investigations or analysis only.
User training	Training for individuals responsible for distribution of identification cards, monitoring of the system or location data, etc., should be provided by the vendor and/or the school, as appropriate.
Maintenance	Maintenance costs may be associated with the monitoring of software or the maintenance of hardware periodically.
Consumables	Consumables will range according to vendor and may include batteries, identification cards, sensors, etc.
Energy and energy dependency	Data location systems require the use of networks, servers, Internet, and other energy dependent means.

Table 8-7 Location Tracking System Cost Considerations (Continued)

Cost Factor	Cost Description
Software licenses	Monitoring or data retrieval software is usually included with the initial acquisition or installation cost, but may need to be periodically updated with the purchase of new licenses.
System integration	Location systems could conceivably be integrated with security systems such as cameras. Integration costs will vary depending on desired capability, type of system, etc.

8.5.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

RFID and GPS hardware components are expected to become smaller and cheaper in the future. As satellite mapping and computer imagery continue to advance, the capabilities and applications for GPS tracking software do so as well.

Additionally, software apps, such as “Here Comes the Bus,” intended for parents to track their own children, are being launched in some school districts.¹⁴ Central Indiana school districts offered this app starting in the fall of 2015. Parents download it to their phone, tablet, and/or computer. When needed, parents access the app and enter the district code number and their child’s identification number to find the precise location of the bus. The app works by accessing the GPS on board the buses and letting the parents view the precise bus location in real time. Parents can view only their own child’s school bus data. The app also allows the parents to set up an alert system to text them when the bus is close to home. The school bus icon changes to a different color when the bus reaches the school.

8.5.7 VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 8-8 provides some examples of known vendors of location system vendor products; however, it is not comprehensive and other vendors may exist. The list is current as of 3 February 2016.

Table 8-8 Student Location System Vendors

Vendor	Website	Note
Edulog (track students in bus)	www.edulog.com	System for students
Newgate Security	www.newgatesecurity.com	System for students
Omnalink	www.omnilink.com	System for students
RMT	www.rmtracking.com	System for students
Votum Technology Group	www.votumtg.com	System for students
Wherify	www.wherifywireless.com	System for students
Zonar systems (track students in bus)	www.zonar.com	System for students
Fleetmatics	www.fleetmatics.com	System for buses
Newgate Security	www.newgatesecurity.com/case-studies/	System for buses
Synovia Solutions	www.synoviasolutions.com	System for buses
Votum Technology Group	www.votumtg.com	System for buses

¹⁴ <http://fox59.com/2015/07/27/districts-launch-new-school-bus-tracking-app/>

8.6 UNMANNED AERIAL VEHICLES

8.6.1 INTRODUCTION

Any aircraft that does not have an on-board pilot is considered to be an unmanned aerial vehicle or UAV. UAVs are usually controlled by a pilot on the ground who steers the aircraft either by maintaining visual contact or by referring to tracking instruments or visual data transmitted by the UAV. Generally, only military-grade UAVs are capable of flying without human guidance. The following terms are helpful in understanding this subsection:

- **Drone:** For the purpose of this report, drone is a synonym for UAV.
- **UAV:** Unmanned aerial vehicle.
- **UAS:** Unmanned aerial system; used to refer to the UAV and any associated systems, such as navigation or surveillance systems.

8.6.2 HOW THE TECHNOLOGY IS USED

UAVs fitted with cameras have been successfully used in a variety of applications in which an aerial view provides a more effective or safer understanding of the situation, e.g., to observe crop growth (Reference 169) or to search natural disaster sites for survivors (Reference 184).

For schools there is potential for UAVs to be used for mobile video surveillance during mitigation and response efforts on campuses because they allow observation from a distance. For example, UAVs with the ability to stream video to the ground in real time could give law enforcement officers the ability to systematically search for a missing child or reported trespasser; they could provide an aerial view of the crowds at a football game to watch for patterns that might indicate an altercation or fight in the stands.

UAVs can help to indirectly address violent crime by providing aerial views of school buildings and grounds as part of a school safety assessment or when evaluating evacuation and reunification plans. More directly, the use of aerial surveillance may help deter crimes due to risk of detection. A 13-month study found statistically significant reductions in shootings, car thefts, and car break-ins in areas where CCTV cameras were installed (Reference 54). If potential criminals are aware of the presence or possibility of aerial surveillance cameras, a similar deterrent effect can be expected from UAV surveillance.

However, another study suggests that concerns about being filmed may also deter non-criminal actions that a person prefers to keep private, such as going to a counselor or psychiatrist's office (Reference 320). This perception of loss of privacy is an issue that schools must address if UAVs are to be implemented for crime reduction.

8.6.3 WHAT MAKES THE TECHNOLOGY GOOD

8.6.3.1 How the Technology Works

The UAVs likely to be used in a school environment are small, battery-powered aircraft capable of carrying a small video camera. The operator directs the movements of the UAV, and in some cases controls camera functions, using a radio frequency remote control unit.

8.6.3.2 Differentiators

Properly placed surveillance cameras mounted outdoors may provide the same benefits of UAVs fitted with cameras, without the added complications of operating the UAV. However, UAVs enable ad hoc

surveillance in areas not already covered by mounted cameras. They also offer a mobile opportunity to examine a situation from various points of view, which may be critical to developing an appropriate response to a crime in progress.

8.6.3.3 Specifications and Features

The selection of a UAV is usually determined by first considering its intended use. The distance that the vehicle can be flown before losing remote control and the maximum flight time on a battery charge may affect the UAV's effectiveness over a large campus. Ensuring the selected UAV has the appropriate range for the area to be observed is important.

Likewise, if the purpose of the UAV is aerial surveillance of a school campus, selecting the appropriate camera is also important and will drive the selection of a UAV with a suitable carrying capacity. Gimbals are frameworks for mounting, stabilizing, and aiming the camera. The UAV will also need additional equipment if images will be transmitted while flying rather than accessed after the UAV lands. The UAV must have sufficient payload to support the intended camera and accessories. Supporting a larger payload generally requires a larger UAV.

When considering a UAV, design is another distinguishing characteristic. Fixed-wing UAVs (left image in Figure 8-7) look like miniature airplanes with one or more vertical propeller blades that allow the UAV to travel in a forward direction. Rotary-blade UAVs rely on multiple horizontally oriented propeller blades that surround the body of the vehicle and enable the UAV to take off and fly in any direction including straight up much like a helicopter (Reference 348). Four-bladed quadcopters (right image in Figure 8-7) are more common than fixed-wing UAVs because they are more maneuverable and stable, making them easier for a part-time pilot. However, the extra maneuverability may result in reduced flying time because moving additional blades consumes more power (Reference 24).



Figure 8-7 Fixed-Wing UAV¹⁵ and Rotary Blade Quadcopter¹⁶

¹⁵ <http://voices.nationalgeographic.com/2013/11/30/so-you-want-to-fly-drones/>

¹⁶ <http://www.dohenydrone.com/the-drone-for-you-fixed-wing-versus-rotary-wing>

8.6.3.4 Effectiveness

Colleges and universities are expressing interest in using UAVs to enhance student safety by allowing safety officers to observe areas not easily patrolled in traditional ways. No instances of a public school using UAVs for student safety were uncovered during the research for this study. However, one author concludes that public schools will also implement the use of UAVs if they are found to be effective on college campuses (Reference 179).

8.6.3.5 Policy Impacts

School policies should be modified to specify the acceptable uses of UAVs to collect school surveillance video and to define how the files are used and stored.

The Federal Aviation Administration (FAA) has oversight responsibility for the safe operation of passenger and unmanned aircraft and avoiding conflicts in shared airspace. Under a phased approach, the first rule, Operation and Certification of Small Unmanned Aircraft Systems (Reference 114), is proposed to restrict the flight of unmanned aircraft under 55 pounds to daylight, line-of-sight usage, with a maximum altitude of 500 feet. The requirement for the operator to be able to see the drone and requirements to meet various training certifications could limit the adoption of drones for school safety. The lag between interest and adoption may be the result of schools waiting until the FAA finalizes rules controlling the use of small UAVs.

8.6.4 CONCERNS ABOUT THE TECHNOLOGY

8.6.4.1 General Discussion (What It Does Not Do)

Although UAVs offer the potential to monitor situations from a safe distance and can provide a different perspective that may offer critical safety information, collecting useful data requires a trained operator and analysis of the resulting video files. Unless the video is streamed live, there is a lag between when the event is recorded and the data are analyzed.

8.6.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

While flying, and particularly while hovering, a UAV is susceptible to damage from projectiles fired or thrown at it. In addition to the potential for loss of the UAV and any on-board data, there is the possibility of injury if the aircraft falls onto a person. To prevent unauthorized use or theft, the UAV should be kept out of reach of people while flying, and it must be secured when not in use.

8.6.4.3 Possibilities for Misuse

Because drones can observe people without their consent, there are concerns about operators using them inappropriately. Citing privacy and safety concerns, the University of Arkansas has issued its own ban on UAVs flying over the campus (Reference 52). It is also possible that UAVs operating without secure control signals may be hijacked if someone has the ability to send false GPS signals to the UAV, a process called spoofing, which was demonstrated by a University of Texas at Austin research team (Reference 180). Currently, spoofing a GPS signal requires complex software and expense, making it unlikely that persons other than security staff will gain access to a UAV while it is in use.

8.6.4.4 Liability and Safety Concerns

The FAA reported 25 incidents of small drones nearly crashing into piloted aircraft during a 5-month period (Reference 381). The Consumer Electronics Association estimated about 700,000 drones were shipped in the United States during 2015, which is 63% more than in 2014 (Reference 280). With this tremendous increase in interest in recreational UAVs, there is increased potential for in-air collisions with passenger aircraft, buildings, and power lines, and injury to people or animals on the ground as the UAV lands or takes off. These are issues that the FAA's proposed Small UAV rule (see Subsection 8.6.3.5) attempts to address.

8.6.4.5 Privacy Concerns

Like all files produced by a school, UAV video may be subject to requests for information under the FOIA. Rights of people who reasonably expected their actions to be private but were captured on video must be protected.

8.6.4.6 Accommodations Needed for Disabilities

The use of UAVs should not require accommodations; however, efforts should be taken to ensure anyone entering an area under surveillance is alerted to the use of the cameras.

8.6.4.7 Other Issues

Retrieving or redacting video in the event of an FOIA request could become an unexpected burden.

8.6.4.8 Policy concerns

In 2015, the FAA heard public comments on a proposed framework of Federal regulations controlling the use of small UAVs (Reference 109). An article about current state legislation stated that 45 states considered 156 bills related to drones in the first 8 months of 2015 (Reference 241). With regulations under development, a careful and thorough understanding of all current and proposed Federal, state, and local regulations is necessary to avoid operating a UAV illegally. For example, Hood College in Frederick, Maryland, was required to file for an exemption to be allowed to fly a UAV over the campus because it is within 5 miles of a local airport (Reference 25).

8.6.5 COST CONSIDERATIONS

UAVs fitted with visible light video cameras are relatively inexpensive. Hood College recently purchased a drone with the intention of capturing aerial photographs and video for marketing purposes. The drone and camera were purchased for approximately \$1400 (Reference 25). UAVs with IR video cameras cost substantially more at \$5000 to \$10,000.

No data were found as to the reliability of small UAVs over time. With the relatively small cost of the aircraft and the rapid changes in camera capabilities, it may be reasonable to plan to replace equipment rather than repair it.

One cost associated with all surveillance video is the effort needed to review the video either in real time or after an event. This effort can be extremely labor intensive and thus expensive. Like any video, data and files collected by UAVs may be subject to requests for information under the FOIA. In the event of an FOIA request, the effort to review the video files and provide the requested information can be extremely labor intensive, resulting in unanticipated costs.

As with all video camera systems, there is a cost associated with storage of the large files. Many schools opt for a cloud storage provider that allows for capacity to be purchased as needed, rather than purchasing and maintaining local storage. Table 8-9 list some cost considerations to take into account when considering the purchase of UAVs.

Table 8-9 UAV Cost Considerations

Cost Factors	Cost Description
Acquisition	Varies widely based on payload; non-military UAVs with cameras were found to cost from under \$100 to more than \$30,000. Initial hardware costs include cameras, remote controls, gimbals, and other accessories.
Installation	None
Operation and labor	Varies with surveillance needs. This technology requires real-time operation and may also involve some additional effort to enhance, analyze, or manipulate video files.
User training	Varies with the complexity of the UAV and camera. At a minimum, operators must learn to fly the UAV safely and effectively to capture useful data.
Maintenance	Varies with use; preparation includes replacing batteries and media. Some parts are user replaceable, whereas others may require factory repair.
Consumables	Varies. Rechargeable batteries have a finite number of times they can be charged. The purchase cost can range from a few to hundreds of dollars. Electronic media must be also replaced periodically to ensure full performance.
Energy and energy dependency	Varies with use; batteries must be recharged for each operation.
Software licenses	None identified, but some systems may include software to enhance, redact (such as blurring faces) or otherwise manage digital video files.
System integration	Varies. Original video files must be stored on a secure drive according to school retention policy.

8.6.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

The increasing public interest in flying UAVs is likely to drive changes in the technologies of the vehicles themselves as well as the cameras and controls associated with them. Supply and demand may drive prices down. Wireless Internet links between aerial cameras and ground-based monitors may make real-time monitoring of surveillance video more efficient. Continued developments in small batteries and more efficient flight may also increase flight durations (Reference 51). However, UAV use for K-12 school security surveillance is unlikely to have widespread adoption until privacy and safety issues associated with the technology are worked out in other domains, such as commercial events and college campuses.

8.6.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 8-10 provides examples of known vendors of non-military UAVs; it is not comprehensive and other vendors may exist. The list is current as of 15 October 2015.

Table 8-10 UAV Vendors

Vendor	Website	Notes
DJI	http://www.dji.com	Drones, cameras, accessories
DSLR Pros	http://www.dslrpros.com/dslrpros-products/thermal-aerial-drone-kit.html	Drones and cameras
Microdrones	http://www.microdrones.com/en/home/	Drones, cameras, accessories. Site includes numerous use cases
PrecisionHawk	http://www.precisionhawk.com	Drones with variety of specialized sensors
XFold	http://xfoldrig.com/	Drones must be purchased from an authorized reseller (listed on site)

8.6.8 FURTHER READING

For additional information, consult:

- <http://www.faa.gov/uas/>, which includes information about the legal operation of UAVs in the United States, such as flight regulations and UAV pilot certification requirements.

8.7 CONCLUSIONS

This chapter discussed several surveillance technologies, from video cameras, which are rather prolific in today's society, to gunshot detection systems, which are relatively new. Also covered were location technologies (specifically RFID and GPS) and UAVs. The goal is to inform school officials of the possibilities provided using today's technologies. The solution for any given situation is unique and may incorporate one or more of these capabilities.

This page intentionally left blank.

Chapter 9. TECHNOLOGY REVIEW – WEAPONS DETECTION

Morgan F. Gaither, MS

9.1 INTRODUCTION

Weapons detection systems are designed to detect weapons concealed on persons or in their belongings. Depending on the technology employed, these devices can detect metallic, organic, or explosive objects. Additionally, they can detect weapons in mass (large) or trace (minute) quantities. For the purposes of this report, the research team focused on systems designed to detect weapons such as firearms, knives, and explosive devices carried by a person or in his/her personal effects.

It is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district prior to purchasing a safety or security technology. Table 9-1 presents the means by which the study team evaluated weapons detection system capabilities, aligned with the Federal Emergency Management Agency (FEMA) mission areas: Prevention, Protection, Mitigation, Response and Recovery.¹ This assessment combines the opinion of security subject matter experts and the informed judgment of the authors who evaluated the technologies. Reviewing this table provides a summary of the areas of school security and safety for which weapons detection systems may be best suited.

¹ The preparedness cycle consists of the following five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.
- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

Table 9-1 Weapons Detection Systems – Technology Impact Summary

Technology	Prevention	Protection	Mitigation	Response	Recovery
Personnel Systems					
Metal Detector	HIGH Personnel weapons detection systems provide deterrent impact and facilitate identification of contraband on individuals	HIGH School officials may be able to remove threats and identify problem individuals before incidents occur	NONE No significant impact on mitigation was noted	NONE No significant impact on response was noted	NONE No significant impact on recovery was noted
Baggage Systems					
X-ray baggage screening system	HIGH Baggage screening systems provide deterrent impact and facilitate identification of contraband in baggage	HIGH School officials may be able to remove threats and identify problem individuals before incidents occur	NONE No significant impact on mitigation was noted	NONE No significant impact on response was noted	NONE No significant impact on recovery was noted.
<p>Impacts as they relate to a technology's ability to impact a school's ability to <i>prevent, protect, mitigate, respond, or recover</i> from an incident.</p> <p>High: Technology is expected to have a <i>significant</i> impact.</p> <p>Medium: Technology is expected to have <i>some</i> impact.</p> <p>Low: Technology is expected to have <i>little</i> impact.</p> <p>None: Technology is expected to have <i>no</i> impact.</p> <p>Caution: Technology will have an impact; however, it may also have unintended consequences.</p>					

Further details about these weapons detections systems are provided in Sections 9.3 and 9.4.

9.2 UTILIZATION STATISTICS

No comprehensive utilization statistics were identified for the use of weapons detection systems in schools, however the National School Safety and Security Services, an Ohio-based national school safety consulting firm, notes the following: "While there are no credible statistics on the exact number of schools using metal detectors, stationary metal detectors used on a daily basis are typically limited to large urban school districts with a chronic history of weapons-related offenses. U.S. schools regularly using stationary metal detectors on a day-to-day basis are the exception, not the rule."²

² <http://www.schoolsecurity.org/trends/school-metal-detectors/>

9.3 PERSONNEL SYSTEMS

9.3.1 INTRODUCTION

Personnel weapons detection systems (i.e., those designed to detect weapons on people) are deployed in a wide variety of private and government facilities nationwide including airports, government offices, banks, and schools. A widely used type of personnel weapons detection system is a portable and/or handheld metal detector which is used primarily to locate undesirable objects (such as guns and knives) containing conductive materials that are hidden on a person's body. Walkthrough portals, often supplemented with separate baggage screening, are another option for scanning people (Figure 9-1).



Figure 9-1 Examples of Personnel and Baggage Screening Areas^{3, 4}

Although there are other types of personnel detection systems in use in other facilities like airports (e.g., millimeter wave, x-ray backscatter, x-ray forward scatter whole body imaging systems), no examples of the use of these systems in schools were identified by the research team. This section focuses mainly on the use of metal detector systems; however, as other technologies mature and become more mainstream, they may become viable options for deployment in schools.

9.3.2 HOW THE TECHNOLOGY IS USED

There are two or three common ways the technology is typically set up and used. In many instances, a portal system (e.g., one in which persons walk through the detector) is permanently installed at or near the entry point to the building. Building entrants are required to pass through the portal before or immediately upon entering the school. Alternatively, handheld devices may be set up in “stations” or near tables or other cueing areas and used to scan all or part of the entering population.

Accordingly, administrators and security staff should consider the following factors:

- Handheld or fixed systems: Handheld systems may require fewer personnel (per system) and, because they are mobile, are easily deployed in temporary situations. Fixed systems often have higher throughput rates.

³ <http://www.thetruthaboutguns.com/2012/09/daniel-zimmerman/quote-of-the-day-every-additional-penny-edition/school-metal-detector-courtesy-businessinsider-com/>

⁴ www.kansascity.com

- Deployment location: If all students and staff will be screened, all individuals will need to be directed toward the entrance(s) that have available screening devices, and other entrances (such as doors and even windows) will need to be secured to ensure no weapons are passed through them.
- Set of individuals to be screened: Students only, everyone entering the school, or just visitors? The number of people being screened (visitors only, the students, or everyone entering the school) will aid in identifying the amount of staff and systems that need to be devoted to the weapons detection effort.
- Frequency of screening: A recommendation in *Campus Safety Magazine* (Reference 153) states: “When [weapon] checks are conducted regularly and at the same location, K-12 students in particular often find ways to circumvent the process. It is for this reason Mike Dorn, executive director for Safe Havens International, recommends the random deployment of metal detectors.” Whether deployed randomly or not, identifying when to screen also aids in identifying necessary resources and developing screening procedures.
- Events on school property: Consider if screening will be deployed at special school events such as assemblies, dances, or sporting events.
- Supporting procedures and policies: If individuals set off the detector after they have voluntarily divested themselves of metallic objects, are they subject to additional searches? Will pat downs ever be used, and if so, where will they occur and what are the procedures and policies for them?
- Operation and Maintenance: Will screening be conducted by armed law enforcement, school resource officers, administrators, etc.? Do the designated operators have the proper training and necessary authorities for these duties and the possibility of finding a weapon? How is the technology calibrated? Are there any routine tests needed to ensure proper operation?

This list of factors is not comprehensive, nor does it take into account local or state laws, school or school district policies, local social or political sensitivities, or even school-specific designs and layouts. However, taking operational, procedural, and administrative factors such as these into consideration can serve as a guide to purchasing or deploying walk-through and whole-body metal detectors or their handheld counterparts in a school environment.

9.3.3 WHAT MAKES THE TECHNOLOGY GOOD?

9.3.3.1 How the Technology Works

A 1999 U.S. Department of Justice (DOJ) Office of Justice Programs and National Institute of Justice (NIJ) report (Reference 139) gives a general overview of the technical operations of metal detection technology. At a high level,

A metal detector actually detects any conductive material—anything that will conduct an electrical current. The typical pulsed-field portal metal detectors generate electro-magnetic pulses that produce very small electrical currents in conductive metal objects within the portal archway which, in turn, generate their own magnetic field. The receiver portion of a portal metal detector can detect this rapidly decaying magnetic field during the time between the transmitted pulses. This type of weapon detection device is "active" in that it generates a magnetic field that actively looks for suspicious materials or objects.

Theoretically, then, a metal detector can detect any material that can conduct and create a magnetic field, but will not detect any material (including some types of metal) that do not have these properties. Additionally, note that the magnetic fields generated must be of a certain magnitude to be detected by the equipment (settings on this equipment “sensitivity” vary by manufacturer).

9.3.3.2 Differentiators

These systems are not designed for use with baggage or parcels, only people. Baggage screening (discussed in Section 9.4) should be accomplished using different means.

In addition to these factors, potential lower-cost solutions should be considered, such as random (handheld) metal detector sweeps, which can serve as real-time opportunities for weapons detection as well as a strong deterrent against bringing weapons to school.

9.3.3.3 Specifications and Features

While essentially all walk-through metal detectors function in the way previously described, there are a number of options, capabilities, and features offered:

- **Weather protection:** Due to their physical design or layout, some systems include greater protection against the elements (for protection of the system electronics against rain in outdoor environment).
- **Single or dual detection:** Provides scanning for either one or both directions and sides of the metal detector portal. Dual detection allows for better magnetic field uniformity and detection performance.
- **Specialized zone indicators and lighting:** System lighting can indicate which area of the body an object is being detected (e.g., head, torso, or legs).
- **Random alarm functions:** These functions are available by many vendors and can be set to (purposefully) randomly alarm on a given percentage of the population who may not otherwise cause an alarm. This function allows for purposeful randomized screening and can be used as a deterrent or to potentially detect other prohibited items.
- **Traffic counters:** These sensors count the number of individuals passing through the system.
- **Interference suppression:** System coils can be shielded in such a way as to minimize the “noise” caused by other nearby systems (such as x-ray baggage screening). Minimizing this noise reduces the rate of false or nuisance alarms.
- **Specialized controls and access functions:** Systems can be designed such that they require dual locks or access codes, which prevents tampering with or accidental modifications to the program or system. Access control functions and security settings will vary by manufacturer model and should be a factor in considering which model(s) are ultimately purchased.

Handheld metal detectors come in varying sizes, but generally have a more limited range of options, capabilities, and features:

- **Sensitivity setting:** Models vary in their sensitivity to the types of materials they detect including ferrous, non-ferrous, stainless steel, and other metal objects.
- **Calibration:** Metal detectors need periodic calibration to perform accurate detection; many models include options for self- or automatic calibrations, which decreases the amount of downtime during operations.

- **Detector design:** Due to the extended nature of operations of some metal detector uses (e.g., multiple-hour shifts of screening operations), many models have ergonomic design features. Additionally, the types, sizes, and locations of on/off switches and other buttons may vary.
- **Alarm type:** To facilitate detection in loud, covert, or other types of operations, vendors often offer various alarm types for their systems including audible, visual, and tactile (vibration).

9.3.3.4 Effectiveness

Metal detection technology has been used for personnel weapons detection for decades. As the DOJ report notes: “Metal detectors work very well—they are considered a mature technology and can accurately detect the presence of most types of firearms and knives. However, metal detectors work very poorly if the user is not aware of their limitations before beginning a weapons detection program and is not prepared for the amount of trained and motivated manpower required to operate these devices successfully.” (Reference 139) In addition, a well thought out response procedure covering secondary screening (any screening or searches that occurs after an individual creates an alarm on the primary screening device (e.g., metal detector)) and detection of a weapon is essential to ensure consistent use of the system.

NIJ published draft voluntary standards for handheld metal detectors (NIJ Standard 0602.03) and walk-through metal detectors (NIJ Standard 0601.03). These voluntary performance standards and an associated document “Public Safety Selection and Application Guide to Walk-Through Metal Detectors (NIJ Guide-0601.03)” are produced as a part of the Standards and Testing Program of the U.S. DOJ and define performance requirements and test methods for metal detection devices. Whether or not these standards are used in the selection of a particular school’s detection devices, all schools should consider the following factors:

- **Detection capability:** Systems often have variable detection settings. While it may seem obvious that higher sensitivity settings allow for the detection of smaller (more easily concealed) weapons, these higher sensitivity settings often are accompanied by increased nuisance alarms rates. Note that these higher settings do not increase any potential concern about radiation exposure.
- **Maintenance factors:** Each system vendor may have different recommendations on maintenance, calibration, etc. Those systems that continue to have acceptable detection capability while needing minimal maintenance and downtime are more desirable.

9.3.3.5 Policy Impacts

Implementation of this technology may be controversial due to Fourth Amendment prohibitions against unreasonable searches and seizures. In addition, the potential need to block or deny access to other entrances during their use means any Federal, state, and/or local fire laws pertaining to building access and safety must be taken into consideration. Closed entrance doors must continue to be accessible as a means of egress. Additionally, many implementation decisions may be impacted by issues of budget and civil liberties so school policies and procedures should be carefully considered and clearly written.

9.3.4 CONCERNS ABOUT THE TECHNOLOGY

9.3.4.1 General Discussion (What It Does Not Do)

Metal detection systems can be best categorized as “anomaly detectors,” i.e., they do not identify weapons, only certain masses and configurations of metallic materials. These systems cannot distinguish, for instance, between a gun, a cellular phone, and a large metal belt buckle. Any alarm or alert generated by these systems will require follow up by security personnel according to pre-established procedures (e.g., voluntary divestment of the article, pat down). Additionally, non-metallic weapons and explosive materials without a significant metallic content will go undetected during screening. If these items are a security concern, alternative technologies and/or policies should be considered.

Metal detection devices are effective at individually scanning people or objects that can be passed through the detection area of the device, but they are of limited use in searching large areas for weapons.

9.3.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

The use of metal detectors will not prevent weapons from being passed through other open doors, windows, or other avenues for entrance into the school. As noted in *The Atlanta Journal-Constitution* (Reference 255): “Only two days after Grady High School officials moved from random checks to the labor-intensive screenings at the doors, a student bypassed security safeguards by opening a gym door for Morgan Tukes, a 17-year-old with a troubled past and a pink .380-caliber pistol in her left pocket. The gun went off, shooting her in the leg.” Depending on how, when, and where they are deployed, school officials and administrators will need to be aware of this vulnerability (e.g., someone leaving a weapon in a vehicle until later in the day or passing it through another entrance) when planning for the use of the technology.

9.3.4.3 Possibilities for Misuse

Although a checkpoint provides a potential level of security to the school as a whole, the individuals who staff that checkpoint are vulnerable to attack. As noted in a *Campus Safety Magazine* article (Reference 153): “The gunman responsible for the 2005 Red Lake School shooting, for example, shot the unarmed security guard operating the school’s metal detector before shooting his intended targets—students. To counter this threat, a campus might deploy a roaming armed officer or coordinate with local law enforcement officers.”

9.3.4.4 Liability and Safety Concerns

School officials should consult the standards discussed in Subsection 9.3.3.3 in addition to the specific manufacturer’s guidance on safety concerns of any walk-through or handheld metal detector. In general, because they do not emit ionizing radiation, the electromagnetic fields of these systems are considered safe for everyday use.⁵ Individuals with medical devices, especially implanted devices, should consult with the manufacturer prior to using a metal detector. Alternative screening methods should be available to those individuals who may have cause for concern about their safety.

⁵ Health Physics Society, <http://hps.org/publicinformation/ate/faqs/securityscreening.html>

9.3.4.5 Privacy Concerns

Walk-through and handheld metal detectors do not take images or collect any private information. There should be no privacy concerns for their use, although any follow-up searches or other procedures (e.g., pat downs) may require consideration for personal privacy.

9.3.4.6 Accommodations Needed for Disabilities

The technology does not perform well when screening devices such as wheelchairs or other medical aids needed by persons with some disabilities. In addition to ensuring Americans with Disabilities Act compliance, procedures are necessary for screening individuals using wheelchairs, who have casts or prosthetics, etc.

9.3.4.7 Other Issues

Although they are used to ensure physically safe environments, metal detectors, particularly stationary walk-through units, may create the impression of a more prison-like environment. This is generally an undesirable aesthetic and a side effect of some school security solutions. In *The Atlanta Journal-Constitution* article previously cited (Reference 255), Atlanta Superintendent Erroll Davis is quoted as saying: “Our schools were not designed to be fortresses. They were designed to be places of learning.”

Metal detectors, like other school security systems and solutions, have vulnerabilities and while they may be useful in detecting weapons on people entering a school, a robust number of resources, policies, and procedures are needed for implementation. As noted by Chief Marquenta Sands, director of safety and security for Atlanta Public Schools: “Metal detectors are effective; however, the detectors are only one piece of the school safety and security puzzle that we must solve.”⁶

9.3.4.8 Policy Concerns

The technology facilitates searching individuals; therefore, review of Federal and state rulings on applicable Fourth Amendment cases should be reviewed and considered to ensure the legality of the search. These policy reviews may need to be conducted at the individual school, school district, or even state level in some cases.

9.3.5 COST CONSIDERATIONS

The purchase price of walk-through metal detectors varies, but generally ranges from approximately \$1800 to \$6500, depending on the number of features. Handheld units are considerably less expensive (less than \$1000). The initial purchase price is not the only cost consideration for deploying metal detection systems in school. Other costs to consider are listed in Table 9-2.

⁶ Op. Cit. Health Physics Society

Table 9-2 Personnel Weapons Detection Systems Cost Considerations

Cost Factor	Cost Description
Acquisition	Approximately \$1800 to \$6500
Installation	Stationary systems will have installation costs associated with preparing the location. Electrical power is required. Handheld detectors will not have this cost.
Personnel and operators	These systems are considered “manned systems” in that they need one (or more) operators to be in place during any screening activities. Often, these operators are law enforcement personnel or other security professionals.
User training	All metal detector operators need appropriate training and experience. This training will need to include training on the specific systems being used and on any related school policies and procedures. This training should be periodically refreshed (and even tested) to ensure consistent use of the systems and policies.
Maintenance	Systems require periodic calibration and require periodic inspection.
Consumables	Unknown
Energy and energy dependency	While the systems do not require substantial amounts of energy, walk-through metal detectors are hardwired systems (in most cases) and require access to electrical power.
Software licenses	None
System integration	These systems are designed only for use on people; therefore, baggage screening may require the purchase of and planning for (placement, procedures, etc.) additional personnel (for bags checked by hand) and/or baggage screening systems.

9.3.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

Technologies that can detect non-metallic weapons (such as ceramic knives) may be desirable. For instance, devices that employ millimeter wave, terahertz, infrared, and other technologies, usually in the form of imaging systems like those currently in use in U.S. airports, may be feasible for use by schools in the future, but will be accompanied by associated problems such as privacy concerns. Although not currently cost effective for deployment in schools, these types of systems may become viable in the future as the technology matures, and may be integrated with other existing technologies like the metal detection systems previously described.

Although canines do not fit within the definition of technology, they are a recognized means of detecting materials such as narcotics and explosive materials. Trained canines have the ability to rapidly sniff a crowd and locate the source of a suspicious scent that they have previously been trained to detect. They may offer an alternative or supplemental method for scanning events which would overwhelm the personnel scanning system.

9.3.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 9-3 provides examples of known vendors of personnel weapons detection systems; however, it is not comprehensive and other vendors may exist. The list is current as of 30 October 2015.

Table 9-3 Personnel Weapons Detection Systems Vendors

Vendor	Website	Notes
CEIA USA	http://www.ceia.net/security/sections.aspx?sec=a	Walk-through devices
Garrett Metal Detectors	http://www.garrett.com/	Walk-through and hand-held devices
L3 Security Detection Systems	http://www.sds.l-3com.com/products/metaldetectors.htm	Walk-through and hand-held devices
Rapiscan Systems	http://www.rapiscansystems.com	Walk-through and hand-held devices

9.4 BAGGAGE SYSTEMS

9.4.1 INTRODUCTION

As discussed in Section 9.3, personnel systems are not designed for to scan the contents of bags, backpacks, purses, boxes, or other objects that may be carried into a school (further referred to in this section as baggage). Although the research team found few examples of baggage detection systems in use in schools in the United States (Reference 14), this subsection describes existing baggage screening options (Figure 9-2) with potential school applications.

Explosive trace detection (ETD) (swipe-and-swab) systems were not found to be in use in schools and therefore are not addressed in detail. Non-technology based means of screening baggage, such as visual inspection by a security professional and canine detection are also outside the scope of this report.

**Figure 9-2 Example of an X-Ray Baggage Screening System**

9.4.2 HOW THE TECHNOLOGY IS USED

Because personnel often enter schools carrying backpacks and other baggage, it is logical that any baggage screening activities (whether using stationary baggage screening systems or using personnel to inspect baggage individually) should be colocated with personnel screening activities and systems because of their complementary screening applications. Baggage screening systems do not screen

personnel, but many of the same considerations noted for personnel weapons detection systems are applicable for baggage screening systems.

When implementing the use of baggage screening systems in school, administrators and security staff should consider the following factors:

- **Types of articles to be detected:** Identifying the thing(s) of interest (e.g. gun, knives, explosives or bomb-related materials, illegal substances) is necessary to determine the best type of system for the job.
- **Who is subject to screening?:** The number of people being screened may correlate closely with the amount of baggage (e.g., backpacks, purses, computer cases) and will aid in identifying the amount of resources (e.g., people, systems) that need to be devoted to the weapons detection effort.
- **Deployment location:** If detectors will not be at every entrance, then all individuals will need to be directed toward the entrance(s) that have available screening devices, and other entrances (such as door and even windows) will need to be secured to ensure no baggage is passed through them that might contain a weapon.
- **Frequency of screening:** Whether deployed randomly or not, identifying when screening will occur also aids in identifying the necessary resources and developing screening procedures.
- **Events on school property:** Consider whether screening will be deployed at special school events such as assemblies, dances, or sporting events.
- **Supporting procedures and policies:** Will personnel be separated from their baggage during the screening process, and if so, for how long? What happens to those individuals whose baggage creates a suspicion or generates an alarm? What further investigation is needed and how will it occur? What is the procedure in the case of a positively identified weapon or explosive device?
- **Operation and maintenance:** Will screening be conducted by armed law enforcement, school resource officers, administrators, etc.? Do the designated operators have the proper training and necessary authorities for these duties and the possibility of finding a weapon? How is the technology calibrated? Are there any routine tests needed to ensure proper operation?

In addition to these factors, consider the potentially lower-cost solutions discussed, such as visual inspection by trained personnel.

The list of considerations is not all-inclusive and does not take into account local or state laws, school or school district policies, local social or political sensitivities, or even school-specific designs and layouts. However, these and a number of operational, procedural, and administrative decisions must be made prior to purchasing or deploying baggage-screening systems in school environments.

9.4.3 WHAT MAKES THE TECHNOLOGY GOOD?

9.4.3.1 How the Technology Works

Portal baggage screening systems employ x-ray technology and are in use in all U.S. airports. Because of their higher throughput rates compared to individual baggage inspection, they are an efficient way to screen baggage for contraband items. These systems can provide either single or multiple (usually from different angles) simultaneous x-ray images of baggage as it passes through the device. These images can be colored based on material density and other properties (such as organic material content) to assist operators in differentiating and identifying objects in a given image (Reference 72). Usually, this is done in three colors identifying hard, dense, and metallic materials; organic materials; and plastics or

alloys. Operators are trained to recognize weapons, devices, device components, and other contraband materials even when distributed among everyday school-appropriate items, but this detection ability requires understanding which objects are prohibited on school grounds and experience at identifying them via their x-ray image (instead of their visible light image). Although x-ray baggage systems all operate on the same basic scientific principles, each vendor can provide a number of added features to enhance image quality, increase baggage throughput rates, etc.

9.4.3.2 Differentiators

X-ray baggage screening devices are useful in situations that call for a large number of bags to be screened in a relatively short period of time and are best suited for those cases in which all baggage is being screened (as opposed to randomized screening). The throughput rates of screening are higher than manual inspection by security personnel.

Although canines do not fit within the definition of technology, they are a recognized means of detecting weapons and contraband materials such as narcotics and explosive materials. Most K-9 units used in schools focus primarily on drug detection, with a secondary goal of detecting weapons. However, at least one example of a K-9 unit trained exclusively for weapons detection in schools was identified in Pinellas County, Florida (Reference 273). Canines can be brought in to search areas which may contain hidden weapons, such as athletic fields or individual rooms. For example, in one case when a school resource officer was unable to find a weapon reported by a student, a police dog was brought in and detected pellet guns hidden in the backpacks of two students (Reference 304). In another town, canine units from a local police department searched the school to ensure no other guns were on campus after two students were arrested for having a gun on campus (Reference 342). Similarly, after a landscape worker found a handgun on the grounds of a middle school, canine units searched the grounds for any additional weapons (Reference 107).

9.4.3.3 Specifications and Features

There are several performance factors applicable to baggage screening systems. The following list is not all-inclusive; each school or institution should determine its own performance requirements when selecting detection systems.

X-ray baggage screening systems have the following:

- **Image quality:** Higher quality imaging makes identification of materials of concern more likely, but this higher quality image may require more expensive hardware.
- **Baggage throughput rates:** Generally speaking, the higher the better, but this factor may be limited by operator training and experience because each bag must be viewed by an operator during the screening process.
- **False positives** (in which a non-threat item is identified as a threat): A high number of false positives (especially with devices that have automated target recognition algorithms) may indicate the vendor's technology is not mature, that the device needs calibration, or that the operator needs more experience with the particular device.

9.4.3.4 Effectiveness

The author did not identify any current use of x-ray screening systems use in schools, but these systems are used regularly in U.S. airports. A report based on internal covert system testing was released in 2015, and according to several news outlets including CNN (Reference 41) these tests revealed flaws in

the effectiveness of the system and operator detection capabilities. Additional open-source reports such as one from the Congressional Research Services (Reference 102) highlight the issues and concerns with screening systems, including x-ray baggage systems. Reports such as these are useful resources to consult prior to acquiring baggage screening systems because they highlight issues and concerns that might also apply to the use of the devices in schools including space constraints, budget limitations, and operator performance testing.

9.4.3.5 Policy Impacts

These systems, particularly x-ray baggage screening systems, have the potential to take up a large physical footprint when deployed (e.g., the Rapiscan 618XR HP has a length of approximately 7.5 feet). When coupled with school occupant and visitor queuing and screening efforts, local fire and building codes should be consulted and reviewed. Additionally, because personnel and baggage screening efforts will impact school access, emergency response, and other school procedures and policies, these should be reviewed and updated as necessary to facilitate screening efforts.

9.4.4 CONCERNS ABOUT THE TECHNOLOGY

9.4.4.1 General Discussion (What It Does Not Do)

X-ray baggage screening systems can detect the presence of weapons and explosive device components, but these systems are not completely automatic; they rely on operators to interpret images. They have particular throughput rates (specific to each system and vendor) and require trained operators. Also, if and/or when a weapon or explosive device is detected, the systems do not indicate or facilitate appropriate or safe response guidance. Officials and administrators must determine appropriate school response policies and should do this in conjunction with local first responders.

9.4.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

X-ray systems may be vulnerable to disguised or otherwise concealed items and are highly reliant on operator use and image interpretation. Implementing a comprehensive bag screening or randomized screening process require that external entrances (e.g., windows or alternate doors) be closed to prevent circumvention and increase security. Policies and procedures that stipulate screening under suspicious circumstances may also be effective.

9.4.4.3 Possibilities for Misuse

Intentional misuse could be perpetrated by a disgruntled operator by modifying system settings or simply disregarding indications of contraband. It is also possible that others with physical access to the systems could tamper with the system to interfere with its detection ability, and cyber tampering could be feasible. An unlikely scenario is to attempt to expose nearby personnel to greater than normal amounts of radiation.

9.4.4.4 Liability and Safety Concerns

A 2008 report from the National Institute for Occupational Safety and Health (NIOSH) (Reference 1) evaluated the radiation exposure to Transportation Security Administration (TSA) baggage screeners. Their report had the following findings, which may be relevant to the deployment of such systems in schools:

- Low doses of radiation among baggage screeners were found in most airports. Doses for some of the baggage screeners exceeded the maximum dose for the public.
- Unsafe work practices were observed (such as reaching into [screening] machines to clear bag jams).
- Some [screening] machines were not well maintained (i.e., they had bent curtain rods and missing curtain flaps).
- Most [screening] machines emitted low levels of radiation; a few exceeded regulatory limits.

As indicated by the report, x-ray exposure should be routinely checked and measured, and system operators should wear personal radiation dosimeters when operating x-ray baggage screening devices. Strict operating procedures should be in place for any kind of screening system to prevent safety accidents or system misuse.

Additionally, as with personnel screening systems, these technologies facilitate searching individuals' property; therefore, review of Federal and state rulings on applicable Fourth Amendment cases should be conducted and considered to ensure the legality of any searches and procedures.

9.4.4.5 Privacy Concerns

Baggage screening systems collect no personal or private information, but discretion may be appropriate given that x-ray inspections (and searches conducted by personnel) reveal all or parts of the contents of an individual's bag(s).

9.4.4.6 Accommodations Needed for Disabilities

Although wheelchair bound students and some others may need assistance loading bags onto x-ray baggage screening belts, there are no other identified accommodations for these systems. Consideration should be given as to how mobility assistance devices will be screened.

9.4.4.7 Other Issues

No additional issues were identified by the authors.

9.4.4.8 Policy Concerns

Both types of baggage screening systems described are considered searches; therefore, any Federal, state, and/or local applicable Fourth Amendment rulings and cases should be considered prior to their implementation and deployment.

9.4.5 COST CONSIDERATIONS

As with personnel screening systems, the purchase price of baggage screening systems varies greatly according to system size and available options and features. X-ray screening systems cost anywhere

from \$20,000 to \$100,000. Their high initial purchase price is not the only cost consideration for deploying baggage screening systems in school. Other costs to consider are listed in Table 9-4.

Table 9-4 Baggage Screening Cost Considerations

Cost Factor	Cost Description
Acquisition	Approximately \$20,000 to \$100,000
Installation	Stationary systems will have installation costs associated with preparing the location. Electrical power is required.
Operation and labor	These systems are considered “manned systems” in that they need one or more operators to be in place during any screening activities. Often, these operators are law enforcement personnel or other security professionals.
User training	All baggage screening operators need appropriate training and experience. This training will need to include training on the specific systems being used and on any related school policies and procedures. This training should be periodically refreshed (and tested) to ensure consistent use of the systems and policies.
Maintenance	X-ray systems need routine maintenance and calibration. In some cases, these can be done by trained school staff, but in others, maintenance may need to be routinely performed by the system vendor(s).
Consumables	Unknown
Energy and energy dependency	Large baggage screening systems can require a significant amount of energy. These systems are hardwired systems (in most cases) and require access to electrical power.
Software licenses	Some vendors may require software licenses for the use of their technology, especially systems with automated or advanced detection algorithms. Verify this possibility with each specific vendor.
System integration	These systems are designed for use on baggage; therefore, screening of the personnel carrying the baggage may require the purchase of and planning for (placement, procedures, etc.) additional systems and resources.

9.4.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

ETD systems (can be either handheld vapor detection (“sniffer”) systems or desktop swab-and-swipe systems that are more applicable for baggage screening applications. Both systems use ion mobility spectrometry (IMS), which ionizes, separates, and then identifies different molecules. Because of the high sensitivity of the IMS technology employed, many hundreds of types of molecules can be identified. For most systems, a library of molecules and materials of common items and items of interest (like those found in narcotics, explosive materials, and drugs) is programmed into the system. When swab samples from bags are read into the machine, molecules that match items of interest and prohibited items in the database create an alarm to alert the system operator. Detection thresholds (how much of a substance must be present to create an alarm) and other library features may vary by vendor.

ETD devices serve a purpose more closely comparable to the use of canines, but can reduce the labor and rotation requirements necessitated by canine “shiftwork.” Additionally, ETD devices, in some cases, can detect the presence of explosive material as well as identify the substance(s) in part or whole. This additional information is valuable to first responders and for forensics purposes.

Additionally, there are other potential technology types available and in development for the purpose of weapons detection (e.g., millimeter wave personnel screening systems) which may become more common options for school safety options in the future.

9.4.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 9-5 provides examples of known vendors of baggage weapons detection systems; however, it is not comprehensive and other vendors may exist. The list is current as of 24 January 2016.

Table 9-5 Baggage Screening Vendors

Vendor	Website
L-3 Security and Detection Systems	http://www.sds.l-3com.com/applications/checked-baggage.htm
Rapiscan Systems	http://www.rapiscansystems.com/en/products/bpi

9.5 CONCLUSION

The weapons detection systems discussed here focus on identifying concealed weapons either on persons (personnel systems) or in their associated baggage (backpacks, purses, etc.). These systems provide school officials a potential capability to prevent or minimize access to weapons in schools, but each technology type is associated with a number of technical and operational factors that should be considered prior to deployment. School officials should carefully weigh capabilities and technical factors (e.g., system footprint and throughput, types of weapons detected, system safety, false alarm rates) against other operational factors such as cost, screening policy, and privacy rights when considering which (if any) of the available systems are appropriate for use in schools. Because of the dynamic nature of the weapons detection market and school security technology market, school officials should periodically review available and emerging systems to identify those that might be best suited for their school applications.

Chapter 10. TECHNOLOGY REVIEW – OTHER TECHNOLOGY SYSTEMS

Lauren A. Brush, MS

10.1 INTRODUCTION

This section includes a few school safety technology options that are not commonly in use in schools. They are included here to provide school safety decision-makers with additional options and strategies that may have a role in a comprehensive safety program.

Cathy Paine, chair of the National Association of School Psychologists' Emergency Assistance Team, says that the chance that “an armed intruder will come in [is] 1 in 2.5 million.” She indicates that rather than focusing on protection against a shooter, a better plan is to balance efforts to ensure physical safety of the campus, such as perimeter fencing and controlled building access, with efforts to address “psychological safety” such as bullying (Reference 145). However, following highly publicized school shooting incidents, the interest in providing ways to protect staff and students from gunfire has grown. Bullet-resistant items, traditionally the domain of members of the military and law enforcement, may provide a measure of personal protection.

Violence in schools may result from a targeted attack against someone the attacker specifically wants to harm or it may be an effort to injure a large number of victims. In either case, preventing or delaying the attacker’s efforts to find targets may slow a potential attack long enough to allow the intended victims to find cover or escape and for law enforcement to end the threat. Privacy film applied to the windows between hallways and classrooms can prevent an intruder from looking into rooms to find potential victims.

It is important to consider the goals and objectives and recognize that there is a suite of options available to the school or district prior to purchasing a safety or security technology. Table 10-1 presents the means by which the study team evaluated other technology capabilities, aligned with the Federal Emergency Management Agency (FEMA) mission areas: Prevention, Protection, Mitigation, Response and Recovery.¹ This assessment combines the opinion of security subject matter experts and the informed judgment of the authors who evaluated the technologies. Reviewing this table provides a summary of the areas of school security and safety for which other technology systems may be best suited.

Table 10-1 Personal Protection Technologies – Technology Impact Summary

Other Technology Systems	Prevention	Protection	Mitigation	Response	Recovery
Bullet-resistant shield	NONE No significant impact on prevention was noted	LOW Offers protection only against intruders with firearms or edged weapons	LOW Provides protection from bullets and edged weapons while staff initiate lock-down procedures	LOW Provides some protection from bullets	NONE No significant impact on recovery was noted

¹ The preparedness cycle consists of the following five mission areas.

- **Prevention** includes “the capabilities necessary to avoid, deter, or stop an imminent crime or threatened or actual mass casualty incident. Prevention is the action schools take to prevent a threatened or actual incident from occurring.” (Reference 355) Prevention is proactive in nature, requiring the appropriate use of technology or other means to receive warning that an incident may occur and take appropriate action. Prevention technology works best when it is highly visible and known to potential offenders or provides sufficient advance warning for successful intervention before a potential offender can execute.
- **Protection** includes “the capabilities to secure schools against acts of violence and manmade or natural disasters. Protection focuses on ongoing actions that protect students, teachers, staff, visitors, networks, and property from a threat or hazard.” (Reference 355) Protection is proactive in nature, requiring the planned, appropriate use of technology to keep an incident from happening. Protection technology must be visible and known to potential offenders and provide substantial assurance to the potential instigator that his or her plans are unlikely to succeed.
- **Mitigation** includes “the capabilities necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.” (Reference 355) Mitigation also means reducing the likelihood that threats and hazards will have their full effect. It is both proactive and reactive in nature. Not every security situation a school faces can be prevented, but technology that allows school officials to mitigate the damage can be very useful. The same technology may stop the incident from happening in the first place.
- **Response** includes “the capabilities necessary to stabilize an emergency once it has already happened or is certain to happen in an unpreventable way; establish a safe and secure environment; save lives and property; and facilitate the transition to recovery.” (Reference 355) Response may have some proactive elements (a plan, or concept, regularly exercised), but it is reactive in nature. Response technologies enable triage, limit further damage, and allow the school to resume normal activities.
- **Recovery** includes “the capabilities necessary to assist schools affected by an event or emergency in restoring the learning environment.” (Reference 355) Recovery is, by its nature, highly reactive. However, certain technologies play key roles in documenting the incident in detail to support prosecution of the responsible individual (Reference 93). This enables school officials to take actions to resume normal activities, conduct an after-action report, and take appropriate actions to prevent similar incidents in the future.

Table 10-1 Personal Protection Technologies – Technology Impact Summary (Continued)

Other Technology Systems	Prevention	Protection	Mitigation	Response	Recovery
Privacy window film	NONE No significant impact on prevention was noted	LOW May prevent intruders from locating potential targets	LOW May prevent intruders from locating potential targets	CAUTION May interfere with first responders' efforts to locate intruders and victims	NONE No significant impact on recovery was noted
<p>Impacts as they relate to a technology's ability to impact a school's ability to <i>prevent, protect, mitigate, respond, or recover</i> from an incident.</p> <p>High: Technology is expected to have a <i>significant</i> impact.</p> <p>Medium: Technology is expected to have <i>some</i> impact.</p> <p>Low: Technology is expected to have <i>little</i> impact.</p> <p>None: Technology is expected to have <i>no</i> impact.</p> <p>Caution: Technology will have an impact; however, it may also have unintended consequences.</p>					

These two personal protection technologies are discussed in greater detail in Sections 10.3 and 10.4 in terms of their range of uses, benefits and vulnerabilities, future trends, costs, and current vendors.

10.2 UTILIZATION STATISTICS

The products discussed in this chapter are available for purchase and are being advertised as school safety products by some vendors; however, the authors were unable to find statistics regarding the use of bullet-resistant shields and privacy window films in schools.

10.3 PERSONAL PROTECTION – BULLET-RESISTANT SHIELDS

10.3.1 INTRODUCTION

Unlike most school safety technologies, the products discussed here are intended to protect only one person at a time from an armed attacker. There are several types of portable bullet-resistant products intended to protect a single individual from projectiles. Some options, such as whiteboards and blankets, are intended to be stored in the classroom and distributed during an emergency. Other options are intended to be carried by the individual throughout the day. These include bullet resistant clipboards, covers for personal electronics, jackets, and inserts for backpacks. The terms *bullet proof* and *bullet resistant* are not interchangeable. It is important to understand the difference between the two terms:

- **Bullet proof:** Capable of preventing penetration by a bullet fired from a firearm. Because the force of a bullet is highly variable depending on factors such as the type of firearm, type of projectile, and distance from muzzle to target, items meant to be *bullet proof* are best described as *bullet resistant*.
- **Bullet resistant:** Capable of preventing penetration by some types of projectiles but may allow penetration when subjected to repeated strikes or to higher powered projectiles. Bullet

resistance should be specified in terms of an accepted standard such as National Institute of Justice (NIJ) 018.01 or American Society for Testing and Materials (ASTM) F-1233.

10.3.2 HOW THE TECHNOLOGY IS USED

The technologies discussed are used in a number of different ways, depending on the configuration of the shield that is selected. For example, garments are worn, whereas whiteboards are held in front of an individual. Each use is discussed in more depth next.

Bullet-resistant whiteboards are intended for use as a teaching aid for day-to-day use. However, during an active shooting incident, they could be used to protect the teacher from bullets while initiating lockdown. Unlike the large classroom whiteboards seen mounted on a wall or those on legs that can be moved around the room, bullet-resistant whiteboards for use as personal shields are small to keep their weight low and may include a handle on the back, as shown in Figure 10-1, to make them easier to hold in position. According to the company that makes them (Hardwire Armor Systems), they are constructed from “material similar to the armor plating in bulletproof vests” and “capable of stopping shots from handguns and shotguns” (Reference 6). The device could also be used for cover by the final person evacuating a room, but the small size does not offer protection to multiple people. Proponents of these devices suggest that because students are familiar with whiteboards, there is no additional fear associated with introducing bullet-resistant whiteboards as part of a school safety program (Reference 276).



Photo: Hardwire Armor Systems²

Figure 10-1 Handle on Back of a Bullet-Resistant Whiteboard

A **bullet-resistant blanket** to provide protection from an active shooter evolved from a protective blanket initially developed to offer shielding from flying debris during a severe storm. Each blanket has a 1.5-mm layer of energy absorbing gel over a 7-mm-thick, high-density polyethylene fiber layer, which is said to provide NIJ Level IIIA protection from gunfire. In the event of a lockdown, students would each drape a blanket over themselves to provide protection from flying bullets. Figure 10-2, shows children under red bullet-resistant blankets during a lockdown drill. To be effective, the blankets must be stored in the classroom in a location easily accessible by the students.

² <http://www.popsci.com/technology/article/2013-01/military-armor-maker-debuts-bulletproof-whiteboard-classroom-protection>



Photos: Bodyguard³

Figure 10-2 Protective Blankets

Personal bullet-resistant shields have been used by law enforcement officers for many years (see Figure 10-3) to protect themselves as they approach vehicles during traffic stops. Public concerns about school shootings have increased interest in providing similar personal protection for students and teachers.



Photo: Impact Armor⁴

Figure 10-3 Bullet-Resistant Clipboard

Bullet-resistant shields intended to provide protection to individual students include a variety of forms such as clipboards, iPad covers, and backpack inserts. Because of the small size of these devices, users must determine the direction from which the threat originates, decide whether to protect their heads or vital organs, and then place the device between the shooter and their bodies. Only the backpack insert can protect a fleeing student without requiring effort to hold it in position. Evacuation plans usually direct people to leave all personal items behind when leaving a threatened area which would counter the benefit of these shields.

³ <http://bodyguardblanket.com/>

⁴ <http://www.impactarmortech.com/product-clipboard.shtml>

Hip-length bullet-resistant jackets are also offered for children. However, because of the unpredictable nature of school violence, the student would need to wear this garment at all times regardless of weather conditions.

10.3.3 WHAT MAKES THE TECHNOLOGY GOOD?

10.3.3.1 How the Technology Works

All of the devices discussed here are intended to protect one person from an armed intruder. These devices prevent a bullet from reaching its intended target. The effectiveness therefore depends on the certified level of bullet resistance as well as the likelihood that an attacked individual will have access to the device and properly use it in an emergency.

10.3.3.1.1 Differentiators

When considering the addition of personal bullet-resistant shields, garments, or blankets to a school safety program, the advantage of purchasing enough of these individual devices to significantly improve student safety should be weighed against the benefits of other safety technologies. While the manufacturers of bullet-resistant products developed for schools promote them as an added layer of protection to be used along with other prevention and protection methods, many school safety experts suggest that safety budgets are better spent on other options. For example, security consultant Gregory Thomas suggests that training school staff to recognize potentially violent students is more effective than bullet-resistant shielding in preventing school shooting casualties (Reference 73).

10.3.3.2 Specifications and Features

When considering the addition of personal shields to complement a school safety program, a primary consideration is the size and weight of the device because this determines how much of the body can be protected and how easily the device can be used in an emergency. A bullet-resistant laptop case could provide coverage for the head or a portion of the torso, but leaves significant critical areas unprotected. However, a larger shield will weigh more and may be difficult for smaller students to carry throughout the school day. Backpack inserts sold by BulletBlocker add 20 ounces to the weight of an existing backpack, which is similar to carrying an additional textbook.

The only examples of bullet-resistant shields found to be in use in schools are bullet-resistant whiteboards. The Colonial School District in New Castle, Delaware, has added bullet-resistant whiteboards to more than 100 classrooms (Reference 276). Each 18×20-inch board weighs less than four pounds and has a handle on the back to make it easier to convert to use as a shield (Figure 10-1). However, even this may be too heavy for some people to hold effectively.

Bullet-resistant jackets are available in a range of sizes to fit small children through adults. Bullet-resistant blankets are currently offered in three sizes (20×36 inches, 23×48 inches, and 26×50 inches), and although the vendor indicates they are lightweight, no weight specifications are included in their online website.

As with any product intended to provide protection from projectiles, it is important to verify the independent test results for any claims of bullet resistance. Schools should consult with local law enforcement to understand the types of weapons used in local crimes and in school shootings around the country to make an informed decision about the level of bullet resistance needed.

10.3.3.3 Effectiveness

Although the research team found no statistics to indicate the effectiveness of bullet-resistant protective devices for students, data related to police officers may be indicative of potential performance in schools. One study concluded that officers shot in the torso while not wearing body armor were 14 times more likely to suffer a fatal injury compared to those who were wearing body armor (Reference 247), suggesting the protective value of bullet-resistant shielding for the body. However, a national survey of body armor use by police officers reported that nearly 60% (306) of the 521 officers shot during the years 1997 to 2006 were killed while wearing body armor. Most deaths were the result of being shot in an area not protected by body armor, such as the head or neck, or in areas where side or shoulder panels connect (Reference 278). These results suggest that although bullet-resistant shields are likely to increase the chance of surviving a bullet strike to a shielded area of the body, there is also a significant risk of injury if a bullet strikes an unshielded area.

The vendor should be able to supply the results of independent tests indicating the standard met by the product. Tests conducted by the manufacturer should not be considered equivalent to certification.

10.3.3.4 Policy Impacts

Some vendors suggest using bullet-resistant shields to strike an attacker as a last resort, but that implies students may use them offensively against other students. Schools should consider how existing policies about weapons on campus would be affected by the products that could be used as a blunt weapon.

If schools use weapons detection systems, it will be necessary to determine policies about shields which may trigger the weapons detection systems due to the density of the components used.

10.3.4 CONCERNS ABOUT THE TECHNOLOGY

10.3.4.1 General Discussion (What It Does Not Do)

Personal-sized bullet-resistant shields may offer peace of mind, but their small size minimizes their effectiveness during a shooting (Reference 73). Bullet-resistant jackets offer full torso protection against penetration by projectiles from the types of weapons they are certified for, but they do not offer protection from the impact associated with a bullet strike. Officers who survived being shot while wearing a bullet-resistant vest indicate that it feels like “being hit with a hammer” and results in significant bruising (Reference 50). Therefore, a child might be incapacitated and at risk of subsequent harm despite the protection from the initial projectile.

Bullet-resistant blankets offer a larger area of protection than small shields, but still must remain between the shooter and the user. Marketing images show students curled on the floor under the blankets (Figure 10-2), but the blankets leave the sides of the body unprotected from a moving assailant.

Although bullet-resistant products probably offer some protection against edged weapons, the certification testing only refers to projectiles. Therefore, no claims can be made for added protection against violence other than active shooters.

10.3.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

By making portable shields small enough to carry throughout the school day, the effective shielding is too small to protect both the head and vital organs. During an emergency evacuation, students and staff

are usually instructed to leave all belongings behind, which may mean that the personal shield is unavailable when needed.

10.3.4.3 Possibilities for Misuse

The authors did not identify instances of misuse of these products. However, because these devices are often very hard, the shields themselves could be used offensively as blunt weapons.

10.3.4.4 Liability and Safety Concerns

Following a violent incident, individuals who did not have personal shielding devices or were injured despite the presence of a device could attribute blame to the school for not providing devices to all students. Perhaps for this reason, school officials in Worcester County, Maryland, refused a donation of whiteboards intended for Pocomoke High School because the donation would not provide one for every classroom in the school system (Reference 312).

10.3.4.5 Privacy Concerns

These physical security options do not involve any collection of personal information.

10.3.4.6 Accommodations Needed for Disabilities

The ability of a user to access and properly use the device should be considered during the selection of personal protective devices. For example, a student in a wheelchair might be unable to retrieve a protective blanket stored in a closet, and a student who requires both hands to maneuver with crutches would likely find it difficult to keep a handheld shield in a protective position.

10.3.4.7 Other Issues

Research indicates that a safe environment is critical to effective teaching and learning (Reference 194). There is concern that the presence of products intended to protect students from school shooters may have a detrimental effect on students' perceptions of school as a safe place by implying the school must be constantly protected from armed invaders (Reference 276). By adding bullet resistance to objects that are a normal part of the school environment, it is less likely the students will perceive such objects as an indication of increased threat of an armed intruder.

Purchasers should consider the manufacturer's warranty as well as the financial viability of the company providing the warranty.

10.3.4.8 Policy Concerns

For school-provided personal bullet-resistant devices, such as whiteboards, schools should clearly document how the number and location of the devices was determined.

10.3.5 COST CONSIDERATIONS

Costs will vary according to the size of the device and the vendor. The whiteboards used in the Colonial School District cost \$400 each (Reference 276), whereas Bodyguard blankets range from about \$1000 to \$1600 depending on the size (Reference 48). BulletBlocker offers bullet-resistant backpack inserts starting around \$100 each, whereas bullet-resistant jackets for children can be purchased for \$750 each.

Because these devices are intended to provide protection for only one person, the number of devices needed to significantly increase school safety will have a critical effect on the total purchase price.

Research conducted at Texas State University indicated that one or two textbooks were sufficient to stop most common handgun bullets, and that assault rifle rounds could be stopped by three to five books (Reference 331). The implication is that students who routinely carry textbooks in their arms or in a backpack may already have protection equivalent to that provided by a bullet-resistant shield.

Table 10-2 summarizes the costs that might be incurred by implementing bullet-resistant products.

Table 10-2 Bullet-Resistant Shields Cost Considerations

Cost Factor	Cost Description
Acquisition	Varies, identified products ranged from approximately \$100 to more than \$1500
Installation	Minimal effort may be needed, such as adding an insert into an existing backpack or replacing the cover on an electronic tablet. Blankets or whiteboards intended to be kept in the classroom may require the installation of a storage area.
Operation and labor	The product must be held or carried while in use.
User training	Varies, but generally requires some introduction to the product and intended uses and periodic hands-on drills to learn how to use it effectively.
Maintenance	Clean and store according to manufacturer's instructions to ensure continued bullet resistance.
Consumables	None
Energy and energy dependency	None
Software licenses	None
System integration	None

10.3.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

Best practices have yet to be established for bullet-resistant personal protective devices used to improve school safety. The authors found independent news articles confirming the addition of bullet resistance whiteboards in some K-12 classrooms, generally provided by donations from the manufacturer or community members. The authors were unable to determine whether any schools have elected to purchase bullet-resistant whiteboards exclusively through the use of school funds.

Research continues to make bullet-resistant materials lighter and more flexible. For example, work at The Johns Hopkins University Applied Physics Laboratory added carbon nanotubes to increase the bullet-resistant properties of Kevlar, a material commonly used in bullet-resistant body armor (Reference 192). Such improvements may make bullet-resistant clothing or shields more beneficial to schools.

The authors found no indication that schools have taken steps to provide any form of personal shields to individuals in any school or district. Products intended to protect individuals are more likely to be purchased by concerned parents for use by their own children. Based on the opinions of school safety leaders (Reference 73), it appears that schools should consider these individual protection devices as a

last resort and dedicate funding for technologies that attempt to prevent violent crime or provide protection for larger numbers of people.

10.3.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 10-3 provides examples of vendors of bullet-resistant personal equipment; however, it is not comprehensive and other vendors may exist. The list is current as of 15 October 2015.

Table 10-3 Bullet-Resistant Shields Vendors

Vendor	Website	Notes
Attachapack	http://attachapack.com	Backpacks and inserts
Bluestone Safety	https://www.bluestonesafety.com/products/clothing	Vests and jackets styled like street apparel
Bodyguard	http://bodyguardblanket.com/index.html	Blankets
Bullet Blocker	http://www.bulletblocker.com	Clothing, backpacks, notebook and tablet covers, backpacks and inserts
Hardwire Armor Systems	http://www.hardwirellc.com	Whiteboards, clipboards, backpack inserts, door coverings

10.3.8 FURTHER READING

For additional information, consult the following institutions:

- National Institute of Justice
 - Active NIJ Standards and Comparative Test Methods
<http://www.nij.gov/topics/technology/standards-testing/pages/active.aspx>
 Includes standards for ballistic-resistant protective materials, body armor, and handheld and walk-through metal detectors
 - Ballistic Resistant Protective Materials NIJ Standard 0108.01
<https://www.ncjrs.gov/pdffiles1/nij/099859.pdf>
 This standard establishes minimum performance requirements and methods of test for ballistic-resistant protective materials.
- Federal Bureau of Investigation – Crime Statistics
 - <https://www.fbi.gov/stats-services/crimestats>
 Includes reports on a variety of crimes, including crime in schools and colleges.
- Bureau of Justice – Indicators of School Crime and Safety
 - <http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5322>

A series of annual reports by the Bureau of Justice Statistics and the National Center for Education Statistics (NCES) on crime and safety at school from the perspectives of students, teachers, and principals. They provide detailed statistical information on the nature of crime in schools, including 23 indicators of crime at school. Topics covered include victimization at school, teacher injury, bullying and cyber-bullying, school conditions, fights, weapons, availability and student use of drugs and alcohol, student perceptions of personal safety at school, and crime at postsecondary institutions.

- National Center for Education Statistics

- <http://nces.ed.gov/>

NCES is the primary Federal entity for collecting and analyzing data related to education.

- ASTM Standard Test Method for Security Glazing Materials and Systems F1233 – 08(2013)

- <http://www.astm.org/Standards/F1233.htm>

ASTM International is one of the largest voluntary standards-developing organizations in the world. They develop technical documents that are the basis for manufacturing, management, procurement, codes, and regulations for dozens of industry sectors.

10.4 PERSONAL PROTECTION – PRIVACY WINDOW FILM

10.4.1 INTRODUCTION

One concern during an active shooter incident is the possibility for an intruder to look through interior windows from the hallway to the classroom to see if anyone is sheltering in the room. According to the ALICE (Alert, Lockdown, Inform, Counter, and Evacuate) Training Institute, 1600 K-12 schools have received training in their ALICE strategy for dealing with an active shooter (Reference 8). According to the ALICE procedure posted by Idaho State University, the lockdown step includes covering the glass on any doors or windows (Reference 162). Removing or permanently covering interior windows to accomplish this task may be detrimental to the well-being of students and staff according to a study that showed the presence of natural light had significant positive effect on academic achievement (Reference 23). Therefore, school safety plans generally direct teachers to cover interior windows temporarily. Methods for covering windows include closing previously installed curtains or blinds, or taping opaque paper over the glass. However, these actions require teachers to perform a task under stress and place themselves in an area where they could be seen by the intruder. Privacy window films cut to fit and then applied to existing windows allow natural light into the room yet prevent someone from looking through the window into the room. This would eliminate the need to cover any windows during a lockdown.

Privacy film may be translucent enough to allow light to pass into the room, but not transparent enough to enable someone to see into the room. Another option is reflective one-way privacy film, which is mirror-like on one side yet allows light into the room. Although fully opaque films exist, they are not likely to be used in schools due to the negative effects on students and staff of blocking natural light.

The following definitions may be useful during this section:

- **Opaque:** A material that blocks the transmission of light.

- **Polyethylene terephthalate (PET):** A form of the polyester used to make clothing, bottles, and window films.
- **Reflective:** A material that causes light to bounce back to an observer's eye, resulting in the observer seeing a reversed image of the originally transmitted light.
- **Transparent:** A material that transmits light, allowing people and objects on the other side to be distinctly seen.
- **Translucent:** A material that allows light to pass through, but that diffuses the light so that people and objects on the opposite side are not clearly visible.

10.4.2 HOW THE TECHNOLOGY IS USED

Privacy film can be applied to any interior glass that would permit someone to view the inside of a classroom, thereby eliminating the need for a teacher to cover the door window during a lockdown. Translucent film and reflective film both allow light into the classroom, but prevent an intruder from seeing in. Translucent film works in any lighting situation, whereas reflective film is only effective if the interior of the classroom is dimmer than the hallway.

10.4.3 WHAT MAKES THE TECHNOLOGY GOOD?

10.4.3.1 How the Technology Works

Window films consist of thin sheets of PET or vinyl. PET is normally transparent, but pigments or metals added during manufacturing can make the material translucent or reflective (Reference 209).

Humans see light that is reflected off an object and back to the observer's eye where it is processed by the brain as an image. Light can pass through both sides of transparent glass equally; thus, viewers on either side can see through a clear window.

Translucent film absorbs or bends some of the light that hits it. Because the light bouncing back is distorted, a person on one side of the film is unable to clearly see something on the other side. Translucent privacy films come in a wide variety of textures, colors, and patterns to allow the user to achieve the desired esthetic (Figure 10-4).



Photo: DecorativeFilm⁵

Figure 10-4 Examples of Translucent Window Films and the Effect on the Ability To See Details Through the Film

There is a direct correlation between distance from the film and the obscuring effect because the farther the light is from its origin by the time it reaches an observer's eyes, the more distorted the light, and thus the image will be. Thus, someone who is very close to the film, as shown in Figure 10-4, will be visible, though not necessarily recognizable, to an observer outside the room, whereas if someone

⁵ <http://www.decorativefilm.com/?gclid=CLjc1oK0r8wCFQkfhgodtVUKyg>

stands back from the film an outside observer may not be able to determine that the person is in the room.

A typical mirror causes all light that hits it to bounce back to the viewer; thus, the viewer sees only the reflected image and cannot see what is behind the mirror. A one-way mirror has a very thin, nearly transparent layer of metal that allows most of the light to pass through but reflects some of the light back in the direction from which it originated. If an observer is in a bright room separated from a dark room by a one-way mirror, the relatively small amount of light passing from the dark room is overwhelmed by the reflected light generated in the bright room; therefore, the viewer sees only his/her reflection. Conversely, for a person in the dark room, the brightly illuminated room is clearly visible through the one-way mirror because there is very little light in the dark room to reflect back; the majority of light received by the observer has reflected off an object in the bright room and returned into the darkened room. Thus, from the darker side the glass functions as a regular window. Like one-way glass, reflective window film is transparent with a thin layer of metal. When applied to a regular window, it creates the effect of a one-way mirror.

10.4.3.2 Differentiators

Window films are not the only means of preventing someone from seeing into the classroom, but they eliminate the need for a conscious action. For example, many schools choose to install shutters or use dark paper to obscure windows. However, closing shutters or applying paper requires additional action to be taken during the lockdown procedure. Translucent privacy film is effective without any effort required. The effectiveness of reflective window film intended to limit vision into a classroom will be affected by the amount of metal in the product as well as the difference between light levels inside and outside the room.

10.4.3.3 Specifications and Features

When using reflective film, the light intensity must be three times greater outside the room to achieve maximum reflective effect (Reference 340). Therefore, when considering this option, schools should evaluate the range of ambient and artificial light during a lockdown. This product will not appear reflective if the hallway and classroom lights are off, nor if the room is flooded with bright light from exterior-facing windows.

Reflective window film reduces the amount of light that will pass into the classroom. When applied to outside-facing windows, it can also reduce solar heat passing into the room. Vendors should be able to provide test values for the reduction of both light and heat.

As indicated earlier, translucent films come in a variety of finishes offering the possibility for incorporating school colors, or color-coding hallways by using color-tinted films.

10.4.3.4 Effectiveness

The authors were unable to identify any literature about schools using privacy film in their safety efforts.

10.4.3.5 Policy Impacts

Policies that prohibit covering windows (Reference 12) would need to be modified to allow installation of privacy films.

10.4.4 CONCERNS ABOUT THE TECHNOLOGY

10.4.4.1 General Discussion (What It Does Not Do)

Privacy films do not prevent an intruder from breaking the glass and thus viewing the interior of the room. Refer to Subsection 3.3.6 for information about bullet-resistant films.

10.4.4.2 Vulnerabilities and Possibilities to Circumvent or Defeat

While translucent film is always effective, reflective film requires the light level outside the protected area to be brighter than the room interior. On overcast days or if an incident happens during the evening, the reflective film may not prevent someone from viewing the room's occupants.

10.4.4.3 Possibilities for Misuse

Someone could turn off the lights in a room so as to commit a violent act without being observed from outside the room.

10.4.4.4 Liability and Safety Concerns

If a school chooses to implement privacy film but is unable to add film to all classrooms at the same time, a school assessment should be conducted to determine that windows in areas with highest risk are treated first.

10.4.4.5 Privacy Concerns

This technology does not involve any collection of personal information.

10.4.4.6 Accommodations Needed for Disabilities

The author did not identify any disability accommodation issues.

10.4.4.7 Other Issues

No additional issues were identified by the author.

10.4.4.8 Policy Concerns

No policy-related concerns were identified by the author.

10.4.5 COST CONSIDERATIONS

Although only one vendor was found to specifically recommend reflective film for school safety, there are multiple sources of privacy film for homes and businesses, including retail hardware stores that offer window films in a range of prices.

Unlike bullet-resistant window film, privacy film does not require any special installation procedures or modifications to the window frames. It can be installed by the user, which results in minimal labor costs associated with installation.

If the film requires special cleaning products or modifications to existing cleaning procedures, these changes could impact facility maintenance costs. Note, however, that if applied to external windows,

this type of film has the added effect of reflecting solar energy, which could provide decreased cooling bills in hot climates but could increase heating costs in cold climates.

Table 10-4 summarizes the typical costs related to implementing privacy window film.

Table 10-4 Privacy Window Film Cost Considerations

Cost Factor	Cost Description
Acquisition	The price of window films varies with the pattern, thickness of the material, and width of the roll or sheet. One vendor lists privacy film prices from \$4 to \$15 per square foot installed (Reference 386). Another vendor lists rolls of 60-inch-wide one-way mirrored privacy film for \$14.25 per linear foot. ⁶
Installation	Minimal: Installation kits are available from film vendors and general retailers such as Amazon for less than \$15 and allow the purchaser to cut film to size and adhere it using a spray bottle of wetting solution and a squeegee.
Operation and labor	None
User training	Staff should be trained to ensure they understand that room lights must be turned off for reflective film to be effective, and that if the difference between light levels inside and outside the room is not high enough, the film may not be reflective.
Maintenance	Minimal, periodic cleaning per manufacturer's information
Consumables	None
Energy and energy dependency	None
Software licenses	None
System integration	None

10.4.6 EMERGING TECHNOLOGIES AND FUTURE CONSIDERATIONS

Privacy film is inexpensive compared to replacement windows, but it remains more expensive than simply covering the window with paper. A privacy window film with bullet resistance would be an interesting product for school safety.

Electrochromic (commonly called “smart”) glass (Reference 388) and window film can change from transparent to translucent by altering an electric current passing through the material. However, these options are currently much more expensive than passive privacy options. If the pricing drops in the future, these options could become more common for school safety.

10.4.7 CURRENT VENDORS

The authors have not evaluated, nor do they endorse, specific vendors or products. Table 10-5 presents examples of known vendors of reflective window film; however, it is not comprehensive and other vendors may exist. The list is current as of 15 October 2015.

⁶ Decorative Films. “SOLYX: Silver –1560 Mirrored Silver. 60” Wide.” Retrieved 3 December 2015 from <http://www.decorativefilm.com/solyx-silver-1560-mirrored-silver-60-wide>.

Table 10-5 Privacy Window Film Vendors

Vendor	Website	Notes
3M	http://solutions.3m.com/wps/portal/3M/en_U.S./Window_Film/Solutions/	Manufactures privacy and security window films
Decorative Films	http://www.decorativefilm.com/	Frosted and reflective films
Global Innovations	http://globalinnovationsco.com	School-specific reflective window film
Smart Tint	http://www.smarttint.com/	Electric film that can be switched between transparent and translucent
Various home improvement stores	Check local listings	Many hardware and home improvement stores sell and install window films

10.4.8 FURTHER READING

For additional information, consult the following institutions:

- National School Safety Center (NSSC)

- <http://www.schoolsafety.us/>

The NSSC was established by Presidential mandate in 1984 by Ronald Reagan as a joint program between the U.S. Departments of Education and Justice. The Center now operates as an independent non-profit organization serving schools and communities worldwide, providing training and technical assistance in the areas of safe school planning and school crime prevention.

- Homeland Security – School Safety

- <http://www.dhs.gov/school-safety>

To enhance school safety, the Department of Homeland Security offers funding, training, and resources for efforts such as providing money for emergency preparedness, training school bus drivers in security, and hardening school buildings' vulnerabilities.

- National Crime Prevention Council – School Safety

- <http://www.ncpc.org/topics/school-safety>

Tips and resources for students, parents, and teachers to help keep America's schools safe.

- U.S. Department of Education – Working to Keep Schools and Communities Safe

- <http://www.ed.gov/school-safety>

The U.S. Department of Education is continuing its work with the U.S. Departments of Justice, Health and Human Services, and Homeland Security to help ensure schools remain

among the safest places in our communities and to provide students the support they need to succeed.

10.5 CONCLUSION

This section includes some school safety technology options not commonly in use in schools. However, they provide school safety decision-makers with options and strategies that may have a role in a comprehensive safety program, particularly when addressing an active-shooter scenario. The bullet-resistant objects discussed—whether clothing, blankets, whiteboards, or other shield type—are intended to protect one person from an armed intruder. Films applied to interior or exterior glass prevent intruders from viewing the interior of the building or classroom. School officials should carefully weigh capabilities and technical factors (e.g., cost per person or per window, storage locations and access, multi-use applicability, and installation time) when considering which (if any) of the available options are appropriate for use in their schools. Because of the dynamic nature of the school security technology market, school officials should periodically review available and emerging systems to identify those that might be best suited for their school applications.

This page intentionally left blank.

Chapter 11. SCHOOL DISTRICT CASE STUDIES

Kelly A. O'Brien, PhD; William R. McDaniel, PhD; and Steven R. Taylor, MPA

11.1 INTRODUCTION

Technology can make schools safer and more secure. For purposes of this report, technology is defined as any device or mechanism applied or installed in schools to prevent, mitigate, or deter criminal acts of violence in the school environment. Examples of safety-related technologies include, but are not limited to, surveillance cameras, communication systems, alarms, door locks and other entry control systems, weapons detection devices, emergency alert systems, protective glass, interior and exterior lighting systems, social media monitoring, and global positioning systems (GPSs).

To understand how school safety technology is deployed, members of the study team attended school safety conferences, spoke with national experts in school safety, and engaged vendors. Another important avenue of research was to engage individuals from representative school districts, with the intent to discern the “ground truth” about what technology is used and how it is used as well as its effectiveness. In this manner, the team undertook one of the goals of this study—to provide a comprehensive overview of the technology being used in the United States and other nations to prevent and mitigate criminal acts of violence in K-12 schools, both public and private.

In synthesizing the information collected during interviews with four school districts into instructive examples, or case studies, this chapter provides concrete examples of school safety technologies deployed in school environments. The authors also intend that the chapter provides a snapshot in time that will allow readers to gain an understanding of the current technology in use, its implementation, and considerations affecting implementation. By providing a profile of the school district and an overview of technologies implemented, the case studies provide context to the use of school safety technologies in real-world settings. None of the security technologies described herein are endorsed by the authors, the districts, the National Criminal Justice Technology Research Test and Evaluation Center, or the National Institute of Justice (NIJ). These case studies are intended to be used by school district representatives when trying to apply what has worked and has not worked for other school districts. They can be used as a lessons-learned repository.

The information provided in this chapter is intended to be used in conjunction with the other chapters of this document. For example, if the case study discusses the benefits of a physical security information management (PSIM) system and why a district decided to implement one, additional information about how that technology is generally used, as well as acquisition considerations, is presented in Chapter 7 (Technology Review – Software Applications). Chapter 2 (School Safety and Security Technology Implementation Planning) can be referenced to gain a greater understanding about matching the solution to the problem and making an informed decision about acquisition of the technology described in the case study. When an implementation choice about surveillance cameras is described in the case study, consulting Chapter 12 (Legal Review) can steer the reader toward information about legal implications in their location.

Section 11.2 discusses the methodology, including the type of information provided as well as site selection rationale, for developing the case studies included in this chapter. Sections 11.3 to 11.6 present the case studies, and Section 11.7 provides some concluding thoughts. Appendix B contains the questions that were used to guide the discussion during case study interviews.

11.2 METHODOLOGY

11.2.1 CASE STUDY RATIONALE

Neither a comprehensive survey nor a random sample was feasible to ascertain the state of safety technology used in the nation's 132,000 schools (Reference 89). Instead, a small non-representative sample of school districts was used. The team determined that the type of information potentially useful to other schools could be collected at the school district level rather than individual school level.

Case studies are used as a tool to facilitate learning on a topic on the part of the reader. The case studies included here portray real-life situations involving decision-making with regard to a common set of interview questions.

It is assumed that school districts with similar demographic factors such as size, geographic region, degree of urbanization, etc., will give rise to similar requirements for protection or school security postures. Interviewing a comparatively small number of school district personnel from a few types of school districts maximized the value of information given the resources available.

11.2.2 STRENGTHS AND LIMITATIONS

The advantages to using case studies are that they illustrate complex concepts. They expose readers to real-life situations that would otherwise be difficult to understand. They allow collection of detailed data that are not easily obtained through other research methods. The many approaches described in a case study can act as a ready reference when readers face similar issues in their own school districts. Lastly, case studies can best illustrate how school districts integrate technologies with each other and with their overall school safety plans. This is intended to help readers place the individual technologies reviewed in this work into context, so that they can consider the relative worth or need for a given technology.

There are some limitations to using case studies, however. It is difficult to obtain appropriate cases that will suit all potential readers. Case studies contain the observations and perceptions of the one person being interviewed and the two people conducting the interview, thus creating the potential for bias in data collection and interpretation. Case studies are time consuming when compared with other methods of data collection such as surveys. It is also difficult to generalize the case study data to a larger population. In many instances, case study data are qualitative, which calls for a different form of data analysis than when using quantitative data. Overall, however, the benefits of conducting case studies, often in conjunction with other research methods, outweigh the disadvantages.

11.2.3 APPROACH

This chapter was developed in conjunction with the Technology Review chapters in that all survey the current state and future path of relevant school safety technologies. By collecting information on these technologies in a single document and using a uniform methodology to review each, the study makes it easier for school safety officials to judge the relative merits of each technology reviewed. To make the analysis more straightforward, the team organized the technologies into categories derived from the broad uses or purposes of technology as implemented for school safety. Items used directly against people, such as weapons, are not considered. Furthermore, because this report focuses on technologies to protect against acts of criminal violence, technologies that address other criminal behavior such as drug use are also not addressed.

Once finished, eight categories emerged:

- Access control: Various locks and barricades, including card access and biometric recognition, intended to restrict or prevent unauthorized entry
- Alarms and sensors: Passive systems, such as entry alarms, and active systems, such as panic buttons, that are intended to notify designated personnel about an unexpected or potentially threatening event
- Communications: One-way and two-way devices for routine or emergency exchange of information within the school or with emergency response personnel
- Lighting: Devices providing illumination that may have a passive deterrence effect or complementary effect (e.g., with cameras) that makes other technologies more effective
- Software: Broad array of software solutions including electronic risk assessment tools, cyber defense capabilities, visitor check databases, tip lines and emergency notification systems, and social media monitoring applications
- Surveillance: Devices that record activities, provide situational awareness of on-scene activities, and enable response to an investigation of criminal activity
- Weapons detection: Devices that detect the presence of weapons on school grounds
- Other Technology Systems: Covers devices that do not fit into the other categories

Information was collected using a structured set of questions to ensure consistency across case studies (see Appendix B). Generally, the intent was to obtain an understanding of the current technologies in use, their implementation, their effectiveness, and considerations affecting implementation. Because these case studies are intended to complement the Technology Chapters, the Case Studies refer to the same eight categories of technologies. Within each category, specific examples of technology were enumerated. For example, within the Access Control category, the team asked about standard door locks, standard window locks, combination locks, padlocks, electronic locks, perimeter fencing, gates, bullet-resistant glass and films, turnstiles, barricades, lockdown systems, mantraps, etc. In addition, demographic information was collected about the district.

11.2.3.1 Selection of School Districts

To select school districts for case studies the research team obtained a number of recommendations for school district candidates during an interview with an executive of Safe Havens International. Additionally, school districts became candidates as a result of Internet searches, vendor recommendations, and those with a history of school shooting incidents.

The researchers sought to ensure there was a wide representation of school districts in terms of geographic distribution, population density, and type of district, but they also wanted to focus on school districts known for using a particular security technology, such as surveillance cameras or metal detectors. The team conducted Internet research, talked with vendors at conferences, and networked with school districts and other subject matter experts to identify ten candidate public school districts by name. To avoid revealing information that could be used to breach security, school districts are referred to by a number. All ten candidate districts, with names removed, are listed in Table 11-1, along with attributes of each district. Note that some districts are large enough to encompass a variety of school types and population densities, and one district covers schools across the U.S. (e.g., in the Northeast, South, Midwest, and West).

Challenges arose in gaining participation by the selected school districts. All participation was voluntary and while efforts were made to minimize the time burden, the Case Studies unfortunately coincided

with the start of a new school year, which may have affected participation. In general, the research team attempted to contact the district-level security officials from ten candidate school districts three times by telephone and three times by email. Four school districts ultimately participated in the case studies. These are labeled District 1, 2, 3, and 4 in Table 11-1.

Table 11-1 Candidate School Districts and Their Attributes

Attribute	District									
	1	2	3	4	5	6	7	8	9	10
Technology										
Metal detectors					X					
Video surveillance	X									
Access control		X								
Alarms and sensors									X	
Datacasting						X				
Social media monitoring								X		
Gunshot detection							X			
PSIM system			X							
Region										
Northeast				X			X			
South	X	X		X				X		X
Midwest				X	X					
West			X	X		X			X	
Population Density*										
Rural	X			X		X		X		
Urban cluster			X	X		X	X	X		
Urbanized area	X	X		X	X	X			X	X
District Type										
Public	X	X	X		X	X	X	X	X	
Private										X
Federal				X						
Tribal				X						

*The Census Bureau identifies two types of urban areas: (1) urbanized areas of 50,000 or more people and (2) urban clusters of at least 2500 and less than 50,000 people. Rural encompasses all population, housing, and territory not included within an urban area. Retrieved 5 February 2016 from <https://www.census.gov/geo/reference/urban-rural.html>.

11.2.3.2 Data Collection

Once the school districts were chosen, structured interviews were conducted with district representatives. All interviews used the same structured approach. There were two interviewers per interview; in general, one interviewer asked the questions while the other wrote down the responses. One district was within driving distance, and therefore the interview could be conducted onsite; the other three were conducted via telephone. Each interview took approximately 90 minutes to complete.

During each interview, participants addressed the following topics:

- Background of interviewee: Position, experience, contact information
- Statement of purpose: Reason for conducting the interview
- Informed consent statement: Consent to be interviewed
- District security planning: Demographics of district, budget and funding, other general safety and security issues
- Featured technology: Closer look at one particular technology
- Detailed technology utilization: Category-by-category discussion of implementation in district; within each category, specific types of technology were discussed (for example: within the weapons detection category, walk through metal detectors, handheld metal detectors, etc.)
- Technology effectiveness: Measuring the effectiveness of deploying technology

11.2.3.3 Data Analysis

Following each interview, the interviewer(s) compiled and reviewed interview notes for accuracy. Data about technologies were categorized and observations noted; each district is presented as a standalone subsection. Each case study addressed the following:

- Description of the school district
- Featured technology driving the case study
- School safety technologies in use
- Integration
- Challenges and concerns

Although interviewees were asked about the effectiveness of technologies, none provided answers to those questions. One discussed the effectiveness of security drills; specific metrics for technology effectiveness were not developed. Because of the small sample size, conclusions about the use of technology cannot be drawn.

11.3 CASE STUDY DISTRICT ONE

11.3.1 DISTRICT DESCRIPTION

The study team interviewed the Security Specialist for the county public schools' Department of Safety and Security. This southern school district serves a mixture of rural and suburban communities. There are nearly 18,000 students enrolled in Pre-Kindergarten through 12th grade. The district operates

17 elementary schools, 4 middle schools, 3 high schools, 1 charter school, 1 alternative learning center, and 1 vocational training center.¹

The district employs about 2150 staff. The district has a 95.5% attendance rate and 93.5% graduation rate.² Student demographic breakdown is provided in Table 11-2.

Table 11-2 District 1 Demographic Distribution

Demographic	Percentage
African-American	18.5
Asian	2.7
Hispanic	5.9
Multi-racial	5.2
Native American	0.4
Pacific Islander	0.2
White	67.2

The district has a budget of about \$214 million that includes local, state, Federal, and other sources of unrestricted and restricted revenue. This revenue covers salaries and benefits, supplies and materials, grounds and buildings maintenance, and transportation. Approximately \$1 million of this budget funds 10 full-time security staff, who provide physical security for middle and high schools in the district. Another source of security funding is through grants and school construction funding. Grants average about \$1.5 million per year; however, this is not a consistent source of funding and can change year to year. A \$400,000 Federal grant following the Sandy Hook incident was used to procure a physical security locking system, but even a small sustainment budget is an issue when implementing technology solutions through grants.

The department has a 5-year strategic plan for identifying and acquiring security upgrades. There are challenges with adhering to it because funding levels and district priorities can change. Moreover, a given grant may restrict what type of equipment may be purchased (e.g., radios when what is really needed—and in the 5-year plan—might be cameras).

Another way the district funds security upgrades is through new construction funding. The security staff works extensively with the building architects to ensure security technologies are integrated early in the design. One example was a new elementary school that incorporated 40 cameras, 23 access-controlled doors (many interior), a panic button for the front office, and a mantrap vestibule area.

In terms of security paradigm, the district employs three different levels of security that align with their elementary, middle, and high schools. The focus for elementary schools is on their main entrance, playgrounds, bus loop, and restroom entrances. The focus for middle schools is the same as elementary schools, with the addition of hallways and cafeterias. The focus for high schools is all of the above, plus parking lots and places where large groups gather such as stadiums and auditoriums.

¹ Details about the school district were obtained from an Internet search conducted on 19 January 2016. The individual representing the school district preferred to remain anonymous.

² Data from 2013 to 2014, the most recent year for which data are available.

There is one person who supervises, maintains, and controls almost 500 cameras, 223 access doors (card readers), 1 visitor management system, and 700 handheld radios.

State law requires emergency plans, and every school has one. Each classroom has a flipchart emergency plan in view; this is transitioning to an electronic version with video clips. Site-specific planning and drills are conducted yearly. State law requires 10 fire drills per year; this has been interpreted as a requirement for 10 drills of all kinds, to include lockdown, earthquake, and severe weather drills. One or two lockdown drills are conducted per year. In cases where the danger is real and not a drill (e.g., a report of a gun at school), the principal or assistant principal is empowered to impose a lockdown. When this actually occurred, a complete lockdown that included a room-to-room search with law enforcement and the sheriff department's canine unit was the result.

Because the district does not have sufficient funds to place a school resource officer (SRO) in every school, one is assigned at each of the three high schools and two are shared across the four middle schools. Every sheriff's deputy has an access pass so he/she can gain access to any school at any time. In addition, the district implemented a partnership with the local sheriff's department called Adopt-a-School. Sheriff's deputies can adopt an elementary school and go into the schools in their off duty time to start early relationships with the children. This has proven very popular with the deputies and the schools.

11.3.2 SCHOOL SAFETY TECHNOLOGIES IN USE

Many technology enhancements started in 2008 when security was established as a separate department in the school district. The first sizable grant was used to establish communications via radios. When selecting technologies, reliability of equipment is a key factor for the district. Currently, the highest priority security technology for acquisition is surveillance cameras.

11.3.2.1 Featured Technology – Surveillance Cameras

The district uses a combination of Panasonic cameras with network video recorders and Aimetis Symphony™ enterprise management software. Schools in the district are widely distributed geographically and each has a local camera surveillance capability. In addition, camera feeds are available in a centralized command center that allows one security operator to view any camera feed (or video playback) from any school on the network. There is a 5-year plan to add cameras and implement video analytics.

Analytics are particularly interesting in that they can be used to prevent and respond to criminal acts in a proactive manner as opposed to using video as a forensics tool. Some key features of the system include virtual fences, scheduling of rules, auto-tracking, and license plate readers. The district sees great utility in the ability to track a person as he/she enters or leaves a playground area; receive an early indication when someone who is on a keep-out list drives into a parking lot; and use other rule-based applications that can create an audible alarm, generate a pop-up alert, send emails, and automatically slew pan-tilt-zoom cameras and lock doors.

Currently, the video system requires two users to be logged on to export video. During account setup, profiles are created so that each school's principal can only see his or her school's camera video. One other use of note was the ability to show video to parents and students; this feature was cited as beneficial for demonstrating or validating claims of misbehavior. Key to privacy concerns is the ability to apply privacy masks on areas of video (e.g., a window or a person moving through a video can be pixelated) when the district must show video to individuals outside the school.

School buses have cameras on board, but they are not integrated with the rest of the video surveillance system; rather, there is a removable hard drive on board the bus from which video can be downloaded. The local transportation department is responsible for these cameras rather than the district's security department.

Table 11-3 presents the implementation aspects of using surveillance video cameras in District 1.

Table 11-3 Implementation Aspects of Surveillance Cameras in District 1

Implementation Aspect	Surveillance Cameras
Acquisition	Cameras, servers, licenses, software, and a network are all required to implement and install a camera system.
Installation	There are significant installation costs and considerations. A great deal of technical knowledge is required to install a network of cameras. Finding a good vendor or integrator is essential if the knowledge is not resident in the district.
Training	The district provides in-house training for security cameras, sometimes contractor-provided. However, the knowledge is fleeting.
Maintenance	Ensuring sufficient budget is available to keep the cameras maintained is essential, and often overlooked.
Power requirements	It is important to consider the power requirements of cameras and servers prior to acquiring them.
Unexpected benefits	The ability to "prove" that a student engaged in a behavior that his or her parent believed was "impossible" is a real benefit to teachers and administrators.
Policies	There are no "dummy" camera mounts (e.g., empty bubbles) out of concern that this can provide a false sense of security. There is no recording of audio in the hallways. Because teachers cannot be recorded due to privacy concerns, there are no recordings in classrooms. Parents cannot view security video without a written request.
Vulnerabilities	
Adaptive behaviors	Students can avoid cameras once they learn their locations.

11.3.2.2 Access Control

Because the district feels that access control is the most effective technology for deterring crime, a variety of strategies are used to control access to the schools. Identocard® is the vendor that provides access control badges. The visitor sign-in software system was developed by the Security Specialist and deployed throughout the district. It rapidly conducts a sex offender check, references local court orders, photographs the visitor, and generates a temporary identification (ID) that must be prominently displayed during the visit.

As a matter of policy, all visitors must enter the school building through the front door and login to the visitor management system. External doors are locked during school hours. School renovation funds are used to add security vestibules to schools during building renovations.

11.3.2.3 Alarms and Sensors

Door position and window position alarms are used throughout the district; glass-break alarms are not. Distress alarm buttons are installed in the front office of each school. When activated, exterior doors are locked.

11.3.2.4 Communications

The school district owns 700 handheld radios. There is also one public safety radio and weather radio in each front office. For mass communication, a cell phone text messaging system is used. There are also 911 alerts, a Google voice number, an afterhours emergency message system, and a landline-based phone tree system. Although intercoms are used, they are becoming outdated and the district intends to acquire an Internet Protocol (IP)-based replacement system.

11.3.2.5 Lighting

Because the high schools serve as community shelters during an emergency, backup generators to maintain key building functions like lighting have been installed. In general, exterior lights remain on; however, some outdoor lights are motion activated. Lights in the parking lots are set on a schedule.

11.3.2.6 Software

Social media monitoring is performed in partnership with the sheriff's department. There is also an incident reporting system that provides a mechanism for students, parents, staff, or others to report a tip via phone, email, text, or web site. All security personnel are issued iPads with student information such as class schedule loaded onto it.

11.3.2.7 Surveillance

Surveillance cameras are addressed at length in Subsection 11.3.2.1.

The district engaged in a demonstration project with the sheriff's department using a drone-based camera; however, there are no plans to purchase drones.

11.3.2.8 Weapons Detection

There are no metal detectors in the district. The district prefers the focus to be on learning, and believes metal detectors may give students a feeling of being in a prison environment, which might negatively impact their learning.

11.3.2.9 Cyber Security

The district employs cyber security including anti-virus software and encryption software.

11.3.3 INTEGRATION

The district is very interested in integrating different systems, but is still in the rudimentary stages of doing so. Because some cameras have pan-tilt-zoom capability, the district anticipates the capability to slew a camera to badge swipes and visitor sign-ins is forthcoming. Integration of alarms and cameras is also an area of interest.

11.3.4 CHALLENGES AND CONCERNS

When prompted as to whether a specific local or national violent incident may have triggered some of the security technologies or protocols, the district representative said there had been no specific incident in the district. Rather, the district is trying to proactively prevent an incident from happening in the first place. According to the district representative, a significant challenge to implementing security technology in schools is that the diverse skills required for the job are not usually possessed by one person. Individuals with a background in law enforcement do not usually have the computer or technology background required to make good purchasing and implementation decisions. Additionally, understanding of the communications devices and systems is needed.

In terms of organizational structure, the district has a separate Information Technology (IT) department that coordinates data storage, servers, and tools. Specifically related to surveillance video, the data are stored for 30 days. From the perspective of the IT department, this requires a lot of storage space and it raises questions as to whether the IT or security department should pay for this storage.

The district is experiencing a significant cultural change as a result of the focus on security; this emphasis manifests as technology and training. A major shift is occurring in personal responsibility for security awareness; i.e., each person in the school system is made aware that the entire security chain is broken when one person does something like prop a door open.

The two biggest hurdles to security technology in the district are reliable and adequate funding and qualified people to run the systems. Currently, the school officials who run the technology are trained for other things (such as administrators) and run the security technology under the umbrella of “other duties as assigned.”

11.3.5 SCHOOL SAFETY TECHNOLOGY LIST

Table 11-4 presents the school safety technologies in District 1.

Table 11-4 School Safety Technologies in Use in District 1

School Safety Technology	In Use	Comments
Access Control – Physical Barriers		
Standard door locks (lock and key); deadbolt	Yes	Some classroom doors lock from outside, some from inside
Standard window locks (latches)	Yes	Many windows do not open; those that do have locks
Combination locks	Yes	On lockers
Padlocks	Yes	On fences
Electronic locks (remotely operated)	Yes	On external access doors; some internal access doors but not classrooms
Perimeter fencing	Yes	
Security or safety personnel	Yes	
Guarded entry gates	No	
Anti-ram vehicle barriers	No	School architecture meant to prevent a vehicle from getting close to building

Table 11-4 School Safety Technologies in Use in District 1 (Continued)

School Safety Technology	In Use	Comments
Bullet-resistant glass; window films	No	
One-way doors	Yes	No outside handles on emergency exits
Turnstiles	No	
Lockdown systems	No	
Mantraps	Yes	
Access Control – Means of ID		
Swipe cards [magnetic or radio frequency identification (RFID)]	Yes	Use proximity MIFARE RFID chip
Temporary ID or visitor badges	Yes	
Staff ID cards	Yes	Combined access and ID card for staff and faculty.
Student ID cards	Yes	Lifetouch photo ID available; but students not tracked.
Access Control – Biometric Readers		
Fingerprint or handprint scanners and readers	Yes	Fingerprints taken for employee and volunteer background checks, not for access control
Iris scanners and readers	No	
Voice recognition	No	
Facial recognition	No	Considering capability as part of video analytics; not purchased yet
Alarms and Sensors – Intrusion and Access Alarms		
Passive infrared (PIR) motion sensors	Yes	For alarms and camera analytics
Photo and laser sensors	No	
Open door or window sensors	Yes	
Millimeter wave motion sensors	No	
Tamper alarms	Yes	Door and window position; no glass-break alarm
Alarms and Sensors – Distress Alarms		
Distress and duress alarms or panic buttons	Yes	Front office; activation locks access doors
Emergency call boxes	Yes	Deployed in partnership with county; 1 box at each high school and one at 1 of the middle schools
Alarms and Sensors – Special and environmental alarms		
Radiological or nuclear	No	
Chemical or biological	No	
Communications – Two-way Communications		
Handheld and vehicle-mounted radios or base stations	Yes	700 across school district.
Police scanners	No	
Cellular telephones (including text messaging)	Yes	Used for mass communication; 911 alerts, Google voice number, after-hours emergency message system
Landline telephones	Yes	Telephone tree system

Table 11-4 School Safety Technologies in Use in District 1 (Continued)

School Safety Technology	In Use	Comments
Intercoms or public address (PA) system	Yes	Becoming outdated; desire an IP system capability
Communications – One-way Communications		
Emergency notification system	Yes	
Mass telephone communication system	Yes	
Instant mass messaging system (text)	Yes	
Automated email system	Yes	
Bullhorns	Yes	Routine use at the schools but not in procedures for security department
Digital signs or billboards	Yes	
Datacasting system	No	
Lighting		
Indoor lights	Yes	High schools are community shelters; generators installed
Outdoor lights	Yes	Some motion activated; parking lots are on schedule; exterior lights in general stay on
Stadium lights	Yes	
Software		
Tip line	Yes	
Risk assessment or management software	No	
Situational awareness software	No	
Security planning software	No	
Violence prediction software	No	
PSIM system	No	Desired capability
Visitor database check software	Yes	In-house application developed
Health or mental health information sharing software	No	
Social media monitoring application	Yes	In partnership with sheriff's department
Text monitoring application	No	Work texts can be monitored
Surveillance		
Standard video cameras	Yes	Digital cameras; some have pan-tilt-zoom capability
Infrared (IR) cameras	No	
Body-worn cameras	No	Need policies first
Smart camera or video analytics	Yes	
Gunshot location system	No	Capability could be useful for large campus
GPS personnel tracking	No	
GPS vehicle tracking	Yes	On buses; radios also deployed on buses

Table 11-4 School Safety Technologies in Use in District 1 (Continued)

School Safety Technology	In Use	Comments
Weapons Detection		
Walk-through metal detectors	No	
Handheld (wand) metal detectors	No	
Radar or millimeter wave weapons detection systems	No	
X-ray scanner	No	
Other Technology Systems		
Bullet-resistant white boards	No	
Pepper spray dispensers	No	
Canines	No	Sheriff's department brings their canines to walk around the buildings; agreement exists with neighboring counties to provide same capability if needed
Safes	Yes	For storing confiscated weapons
Drones	No	
Cyber and Computer Systems		
Computer systems protection	Yes	
Emails (automated email services or messaging)	Yes	There are staff emails sent to work email addresses only
Anti-virus software	Yes	
Encryption software	Yes	

11.4 CASE STUDY DISTRICT TWO

11.4.1 DISTRICT DESCRIPTION³

The study team conducted an interview with a school safety official from an urban/suburban southern school district. More than 111,000 students attend schools in the district. It consists of 11 high schools with average enrollment of about 3000 students, 17 middle schools with average enrollment of about 1500 students, and 53 elementary schools with average enrollment of about 1000 students. Many of the schools are arranged in a campus with an elementary school, a middle school, and a high school sharing common grounds. A new three-school campus is under construction and expected to begin operating in the fall of 2016.

The district employs more than 6500 teachers, resulting in a student-teacher ratio of about 17:1. More than 1400 administrators employed by the district fill roles as principals, counselors, special education specialists, supervisors, curriculum coordinators, and various other support roles. In addition, there are more than 1500 teacher aides and 4000 other support personnel—overall, almost 14,000 employees in the school district.

³ Details about the school district were obtained from an Internet search conducted on 26 October 2015. The individual representing the school district preferred to remain anonymous.

The district has a 95.8% attendance rate and a 50% graduation completion rate⁴. Student demographic breakdown is provided in Table 11-5.

Table 11-5 District 2 Demographic Distribution

Demographic	Percentage
African-American	16.5
Asian	8.6
Hispanic	43.6
Multi-racial	2.3
Native American	0.6
Pacific Islander	0.1
White	28.3

The total budget for the district is more than \$775 million annually, or almost \$7000 per student. The district is growing quickly and has recently issued a \$1.2 billion bond to build new schools and upgrade existing facilities. Of this amount, \$217 million is designated for technology upgrades. About \$55 million of the bond is designated for safety and security. The priorities for this investment are card reader access, video-enabled entry control systems, digital camera additions and upgrades, emergency call buttons, lockdown panic buttons, and bullet-resistant glass at entry points. In addition, \$90 million is allocated for technology infrastructure and instructional technology. Although not specifically dedicated to safety technologies, this infrastructure investment may support safety technologies. To ensure safety technology is well placed and integrated with overall safety plans for the schools, district safety personnel work closely with architects to design safety technologies into new facilities; the same process ensures retrofits of older facilities receive the same benefit.

The school district has its own police department. When it reaches its planned end strength, the department will have 120 officers plus support personnel, or approximately 1 officer per 1000 students. This department replaced a private firm that had been contracted to provide security for schools. All schools have a school safety plan that is drilled regularly. The district also has a school safety coordinator who works with the police department but does not report to the school police chief. This position accounts for all facets of safety, including fire and natural disasters.

11.4.2 SCHOOL SAFETY TECHNOLOGIES IN USE

11.4.2.1 Zonar® Z Pass+™ Parent Notification System⁵

The school district covers 186 square miles and buses approximately 75,000 students per day. To improve situational awareness of the whereabouts of their students while on board buses, the district is conducting an expanded pilot program using the Z Pass+™ system. This system automatically generates a text notification to parents when their children board and disembark from their school bus; it also identifies the bus being ridden, which confirms the child has boarded the correct bus. Each student is issued a unique RFID card that must be presented to an electronic card reader upon entry and prior to exiting the bus. Date, time, and location of the particular student are transmitted to a secure database.

⁴ Data from 2011–2012, the most recent year for which data are available.

⁵ <http://www.zonarsystems.com/solutions/z-pass-plus-parent-app/>, accessed 8 January 2016.

Parents can access this database via an Apple or Google app and receive automatic notification via text or email that their child has boarded or exited the bus.

Administrators see the benefit of the technology in maintaining awareness of a student's location and reducing calls from parents inquiring as to the whereabouts of their child. Parents benefit from instant notification that their child is on or off his or her bus. With the size and volume of bus transportation in the school district, the Z Pass+™ system provides a capability that fills a gap in the district's situational awareness.

11.4.2.2 Access Control

The district locks exterior doors during school hours and is moving to a system with electronic locks and identity card readers in all schools. A system tracks which exterior doors are open or closed, but it is unclear how closely this information is monitored. Classroom doors are secured with standard key locks. After hours, specific exterior doors may be unlocked to accommodate after-school activities. New schools are designed with securable vestibules and video-monitored access control systems. Existing construction is being retrofitted with video-monitored access control and secure vestibules, wherever practical. The district uses Raptor Technologies' "raptor" system⁶ to conduct a check against Federal or state sex offender registries.

The district is installing emergency lockdown buttons in new construction. Although only accessible in a few places in each school, when activated they will automatically lock all exterior doors to control access in case of an emergency. The district representative mentioned that they are interested in fingerprint access technology for police officers to activate and deactivate some locks and systems, such as the emergency lockdown, but have not begun investigating the technology. All windows in new construction are bullet resistant and cannot be opened. Windows at entrances in old construction are being retrofitted with bullet-resistant film, and most also cannot be opened.

The campuses in the district are large and allow open access. Some even have major roads running through or around them. Where there are major roads, the district installs wrought iron fencing to separate the students from the road and serve as a vehicle barrier in case of an accident.

11.4.2.3 Alarms and Sensors

The district uses motion detectors and glass-break detectors during the overnight hours, and all exterior doors have an access sensor connected to the alarm system. The lockdown system in the district can automatically notify the local police department and set off an alarm in the school. In addition, for monitoring athletic facilities such as stadiums, the district uses some PIR detectors connected to an alarm and notification system.

11.4.2.4 Communications

The district police department uses Motorola dual-band P25-compliant digital radios with encryption capability, and has moved away from using a police scanner. Schools in the district currently use Kenwood ultra-high frequency (UHF) analog radios, technology that is nearly 25 years old. Money from the bond issue will be used to update the radio system to digital, ensuring they operate at a frequency that can be monitored by the police radios. Each school will receive a base station, several handsets for administrators, and chargers. The district is building four or five radio towers to ensure the signal from

⁶ <http://www.raptortech.com>, retrieved 8 January 16.

these radios is transmitted across the district. In addition, the district is converting to Voice-over Internet Protocol (VoIP) landline phones, starting with the police department phones.

Existing schools have primarily one-way intercom systems, but each classroom does have a call button to initiate contact with administrators. It is unclear whether new construction will have two-way or one-way intercoms. Most middle and high schools have digital signs placed in lobbies and high traffic areas to communicate events and general information (e.g., weather forecast) with students. Outside of the school buildings, the district is installing emergency call boxes that connect directly to the police department.

The district uses a product called School Messenger⁷ to communicate with parents via text, voice, email, or social media. A county-run tip line service, subscribed to by the student services department, provides students and parents the ability to send anonymous tips that are monitored by the district and local law enforcement.

11.4.2.5 Lighting

All schools are partially lit at night, both interior and exterior, using safety lighting. Some practice fields have lighting, but stadiums are not lit when not in use. Because many of the campuses are near major roads, the grounds are partially lit by streetlights installed for the roads, but this is not a specific part of the safety plan.

11.4.2.6 Software

Although the district is interested in software to integrate security tools, there has been insufficient budget to acquire a PSIM system. Infrastructure improvements associated with the influx of money from the district's bond may facilitate the acquisition and deployment of a variety of electronic security tools.

11.4.2.7 Surveillance

All schools in the district have cameras for video surveillance installed inside and on the exterior of the buildings. Some analog cameras still exist in old construction, but all new schools have digital cameras and older schools are being retrofitted with digital cameras as funding becomes available. As a guiding principle, each high school has about 40 cameras, each middle school about 20, and each elementary school about 10, depending on the school's size and layout. A police department employee works with the district architects on all new construction and retrofits to help place and direct cameras for optimum coverage. The district uses a system to store all video, and this system has some analytic capabilities, but these capabilities are only used when necessary for an investigation. Video may be stored for as little as 7 days, but the technology upgrades coming with the bond issue should extend this time.

The district has investigated a few other surveillance technologies. They recently conducted a pilot test of IR cameras, but concluded the benefit did not outweigh the cost, especially given their investment in video cameras and lighting.

The district also recognizes that body-worn cameras are a potential technology for investigation. However, there are policy and technical issues (e.g., increased video storage requirements) to overcome prior to adoption. There is some interest in gunshot detection technology, but it may not be appropriate for the risks experienced by most of the schools in the district.

⁷ <http://www.schoolmessenger.com>, retrieved 8 January 2016.

11.4.2.8 Weapons Detection

Each high school in the district has two portable walk-through metal detectors. These are used randomly and unannounced at different locations in the school. The process stipulates that all students being screened must leave their belongings and walk through the metal detector, then stay out of the area while the area is searched by officers and canines contracted by the school. Police officers also use handheld metal detector wands and weapon-detecting dogs as backup for the walk-through detectors. Experience from work in a previous school district, where guns were more prevalent, led the district representative to believe that metal detectors have a strong deterrent effect.

11.4.2.9 Cyber Security

The district is not taking extraordinary measures to ensure its cyber security.

11.4.2.10 Other Technology Systems

The district currently contracts canine units for drug and weapons detection, but is planning to create its own canine unit. The unit will initially be focused on drug detection, but may include weapons detection as well.

11.4.3 INTEGRATION

The state requires safety audits and includes reviews of technology integration as part of the audit. The state provides extensive online support and planning tools for these audits. The district has benefitted from a proactive technical director, who planned and integrated much of the current safety technology tools in cooperation with the police department and the school safety official. Having a technical director who invests in school safety and takes an active leadership role in promoting school safety technologies seems to have been one of the foundations of successful technology integration for the district.

One of the integration challenges for the district is software upgrades and versioning. With both new and old software, the district encounters incompatibility with different operating systems. Macintosh and Windows (Version 7) machines are both used by school officials; some older software did not keep up with these operating systems and had to be replaced. Part of the bond funds are being put toward software and hardware upgrades, and it is assumed that any necessary upgrades in safety software will be included in this effort.

11.4.4 CHALLENGES AND CONCERNS

The technologies used by the district, while useful for school safety, come with some issues that must be addressed. Among the most pressing is data transmission and storage. The local bond issue is intended to upgrade the IT infrastructure of the district to help resolve transmission and storage problems, but there does not seem to be a separate accounting for requirements related to safety technologies. None of the servers listed in the technology plan is specifically dedicated to safety-related applications. The transmission towers being installed are for the administrators' radios, not the police band or other communications, even though overtaxed cellular networks and Internet outages were mentioned as concerns.

Video surveillance also carries a separate set of burdens. It is unclear how much of a deterrent the ubiquitous surveillance is on bad behavior and crime. School officials in the district are hopeful that

students are behaving better when they are being filmed, but the real effect is unknown. On the other hand, parents are aware of the surveillance and usually ask for video proof when their child is accused of violent actions. Finding, retrieving, and storing this evidence separately takes time and resources, but does greatly improve the forensics activities of school safety. Ongoing concerns about storing video make it clear these issues constrain the use of safety technologies in some ways.

Another concern mentioned was uninterrupted power supply. The police department building itself is equipped with backup generators powered by natural gas but not every school or campus has such generators. The school district experiences frequent storms and power outages, potentially resulting in safety systems that may be interrupted, reset, or power surged, requiring additional maintenance and resulting in lost coverage.

11.4.5 SCHOOL SAFETY TECHNOLOGY LIST

Table 11-6 presents the school safety technologies in use in District 2.

Table 11-6 School Safety Technologies in Use in District 2

School Safety Technology	In Use	Comments
Access Control – Physical Barriers		
Standard door locks (lock and key); deadbolt	Yes	On classroom doors; do not expect electronic access control on all doors due to numbers. During after-hours events exterior doors are open while the rest of school is locked down.
Standard window locks (latches)	Yes	Not many open.
Combination locks	No	
Padlocks	Yes	Some on exterior gates and service yards.
Electronic locks (remotely operated)	Yes	On exterior doors using card readers and access card; vestibule control on all schools.
Perimeter fencing	Yes	
Security or safety personnel	Yes	
Guarded entry gates	No	
Anti-ram vehicle barriers	Yes	
Bullet-resistant glass; window films	Yes	New construction incorporated; desire retrofit for all front entries of older schools.
One-way doors	Yes	
Turnstiles	Yes	In stadiums only
Lockdown systems	No	Newly constructed schools in future will have button lockdown.
Mantraps	Yes	

Table 11-6 School Safety Technologies in Use in District 2 (Continued)

School Safety Technology	In Use	Comments
Access Control – Means of Identification		
Swipe cards (magnetic or RFID)	Yes	For ID and access control.
Temporary ID or visitor badges	Yes	“Raptor” system in all schools.
Staff ID cards	Yes	
Student ID cards	Yes	Student ID scan upon boarding bus.
Access Control – Biometric Readers		
Fingerprint or handprint scanners and readers	No	Desire capability for SROs to access all schools.
Iris scanners and readers	No	
Voice recognition	No	
Facial recognition	No	
Alarms and Sensors – Intrusion and Access Alarms		
PIR motion sensors	Yes	In some stadiums
Photo and laser sensors	No	
Open door or window sensors	Yes	Building exterior doors have some combination of motion detectors and glass-break sensors.
Millimeter wave motion sensors	No	
Tamper alarms	Yes	
Alarms and Sensors – Distress Alarms		
Distress and duress alarms or panic buttons	Yes	Lockdown system alarms, locks doors, and alerts dispatch.
Emergency call boxes	Yes	
Special and environmental alarms	Yes	Use water sensors in some supply rooms.
Radiological or nuclear	No	
Chemical or biological	No	
Communications – Two-way Communications		
Handheld and vehicle-mounted radios or base stations	Yes	Schools use UHF analog Kenwood radios circa 1988 to 1989; police department uses Motorola P25-compliant dual-band digital radios. New interoperable digital radio system to be acquired.
Police scanners	No	
Cellular telephones (including text messaging)	Yes	
Landline telephones	Yes	Converting to VoIP.
Intercoms or PA system	Yes	Use one-way configuration; every classroom has a call button.
Communications – One-way Communications		
Emergency notification system	Yes	
Mass telephone communication system	Yes	Use School Messenger®; send messages to subscribed groups.

Table 11-6 School Safety Technologies in Use in District 2 (Continued)

School Safety Technology	In Use	Comments
Instant mass messaging system (text)	Yes	
Automated email system	Yes	
Bullhorns	Yes	
Digital signs or billboards	Yes	Installing in lobby and common areas in high schools and middle schools; for messages, weather, breaking news, etc.
Datacasting system	No	Interviewee was not familiar with the term.
Lighting		
Indoor lights	Yes	Partially lit after hours.
Outdoor lights	Yes	Partially lit after hours.
Stadium lights	Yes	Only when in use; practice fields have some lighting.
Software		
Tip line	Yes	Use web site; also app for mobile devices.
Risk assessment or management software	No	
Situational awareness software	No	
Security planning software	No	State required audits, not automated.
Violence prediction software	No	
PSIM system	No	Have interactive PDF (maps, photos); insufficient budget for PSIM system.
Visitor database check software	Yes	Checks national and state sex offenders; does not check for warrants.
Health or mental health information sharing software	No	
Social media monitoring application	No	Desire capability in future; considering three different systems.
Text monitoring application	No	
Surveillance		
Standard video cameras	Yes	Deployed at every school and facility; mix of analog and digital.
IR cameras	No	Previously conducted a pilot; expensive.
Body-worn cameras	No	Under consideration; lack policies, storage requirements, servers, etc.
Smart camera or video analytics	Yes	Hybrid system supports analog and digital; minimal analytics like motion during specified hours.
Gunshot location system	No	
GPS personnel tracking	No	
GPS vehicle tracking	Yes	In all district owned vehicles; parents can receive text when bus approaches residence.

Table 11-6 School Safety Technologies in Use in District 2 (Continued)

School Safety Technology	In Use	Comments
Weapons Detection		
Walk-through metal detectors	Yes	All high schools have two; used randomly, unannounced. Students leave items and walk through; drug-detection dog deployed for failures and items left in room.
Handheld (wand) metal detectors	Yes	
Radar or millimeter wave weapons detection systems	No	
X-ray scanner	No	
Other Technology Systems		
Bullet-resistant white boards	No	
Pepper spray dispensers	No	Officers carry.
Canines	No	Desired capability.
Safes	No	
Drones	No	
Cyber and Computer Systems		
Computer systems protection	Yes	
Emails (automated email services or messaging)	No	
Anti-virus software	Yes	
Encryption software	Yes	Digital radios also have encryption capability.

11.5 CASE STUDY DISTRICT THREE

11.5.1 DISTRICT DESCRIPTION⁸

The study team conducted an interview with the Director of Security and Emergency Planning, who has 26 years of experience in this position. This district is located in a suburban western school district a few miles south of a major metropolitan urban area and encompasses a number of small communities. There are about 15,000 students from Pre-K through grade 12 who attend 13 elementary schools, 4 middle schools, 3 high schools, and 2 K-8 charter schools. The district covers 28 square miles.

The district employs about 840 teachers and 330 instructional aides, resulting in a student-teacher ratio of about 13:1.⁹

The district has a 95.5% attendance rate and 90.7% graduation rate.¹⁰ Student demographic breakdown is provided in Table 11-7.

⁸ Details about the school district were obtained from an Internet search conducted on 13 January 2016. The individual representing the school district preferred to remain anonymous.

⁹ <https://k12.niche.com>; retrieved 13 January 2016.

¹⁰ Data from 2013 to 2014, the most recent year for which data are available.

Table 11-7 District 3 Demographic Distribution

Demographic	Percentage
African-American	1.30
Asian	3.22
Hispanic	17.05
Multi-racial	4.15
Native American	0.45
Pacific Islander	0.12
White	73.70

The district has a budget appropriation of about \$302 million per year for teaching and transporting students, maintaining grounds and buildings, paying salaries and benefits, and providing training. There are two sources of district security funding—the general fund, which fluctuates from year to year, and the operational fund, which is stable. The district-level operational fund covers staff, maintenance, training, and radios; it is currently \$380,000, but increasing. There are eight full-time district security officers who perform patrol and monitoring duties and four part-time dispatchers who are non-patrol security officers. There are also two full-time in-house technicians who install, program, and maintain access control systems, cameras, communication systems, motion detectors, and automated external defibrillators (AEDs); they also serve as trainers for Red-Cross-certified first-aid and AED use and for crisis interventions. Individual high school and middle school budgets cover the cost of 18 campus security supervisors. In addition, there are 14 SROs whose salaries are shared with the police department or sheriff's department. In total, there are 145 employees across the district trained to access the school district security system. This is a point of pride for the district.

The capital reserve fund for security functions ranges from \$100,000 to \$400,000 per year. This funds technology infrastructure and surveillance cameras, among other items. Every 8 to 10 years, a bond election provides major funding for large projects. For example, bond funding from 2002 was used to purchase an integrated security system; current bond funding will be used to continue building out this infrastructure.

Since 2008 there has been a National Incident Management System (NIMS)-compliant, all hazards security plan in every classroom that addresses potential incidents at the school and in the community. In addition, each school has a trained incident command system (ICS) team.

With regard to emergency drills, tabletop exercise drills and lockdown drills are held several times per year. Lessons learned as a result of the drills are shared with schools, and emergency plans are updated annually. Training is also provided.

At the district level, internal and external relationships with professional societies and the local community are important. Examples include local law enforcement, the fire department, the Citizen's Emergency Response Team (CERT), the health department, Boy Scouts, American Red Cross, Federal Bureau of Investigation Infraguard, National Association of School Resource Officers, the state's association of SROs, the National Association of Threat Assessment Professionals, and the state's association of school psychologists.

11.5.2 SCHOOL SAFETY TECHNOLOGIES IN USE

11.5.2.1 Featured Technology – Physical Security Information Management

The district has installed a PSIM system that is intended to filter and extract data from multiple security applications—those that are already installed as well as those that will be acquired in the future—and then correlate and integrate data for decision support through a single user interface. Currently, the technologies that have been integrated into the PSIM include motion detectors, access control, cameras, intercoms, VoIP telephones, and fire detection systems. The director noted that he was very pleased with the system because of the way different technologies and communication systems are brought together in a user-friendly, layered manner.

With the PSIM system, all schools can be managed through the centralized incident command center at one time. Three operators are assigned to an incident command center to prevent operator overload. Because one event can simultaneously impact all schools in the district, the PSIM system needs to be flexible. By creating customized logins and rules, each school can develop its own “view” to meet its requirements. For example, a school can view a map of the school, access points (doors), and security applications. The district can have a different view, customized to create an overview of the entire system. There are currently 145 users with customized PSIM views throughout the district. The director described the way the PSIM system was used during a past incident.

Table 11-8 presents the implementation aspects of using PSIM in District 3.

Table 11-8 Implementation Aspects of PSIM in District 3

Implementation Aspect	Comments
Acquisition	The PSIM system was acquired in 2012, before Sandy Hook. Within 3 months after Sandy Hook in 2013, buzz-in access control features were added.
Installation	System integration is key; having a good integrator or technical staff is essential for effective installation and utilization of the system.
Training	The two full-time technicians received 3 weeks of vendor training. The security officers with monitoring functions receive 2 weeks of on-the-job training.
Power requirements	For devices to be integrated with PSIM, they require power over Ethernet capability; this comes with a cost.
Unexpected benefits	PSIM has the ability to replay an incident; the ability to review actions taken during an incident provides the opportunity to learn from previous actions.
Personnel and culture of security	The culture of security is an issue within the district, but is improving. PSIM reduces risk. Video surveillance, integrated with PSIM, provides more accountability by security officers and staff.
Overcoming	Alarms associated with surveillance video initiate a security patrol.
Adaptive behaviors	Students do not seem to change their behavior when in a camera’s view. However, adults seem to be more aware of the cameras and do modify their behavior. The vandalism rate for after-school hours decreased by 70% to 93% after cameras integrated with PSIM were installed. Cameras deter vandalism and are used to investigate altercations and other undesirable behavior.

11.5.2.2 Access Control

The district employs a variety of access control technologies. Standard door locks with keys are used on exterior doors in older structures; with newer structures, there are either no-key or single-key entries. Interior doors have pushbutton panic locks installed, and window locks are standard. The perimeter fencing and anti-ram vehicle barriers used are blended in with the surrounding architecture. On new construction projects, bullet-resistant window laminates are being used. In addition, lockdown systems are integrated into the PSIM system, and mantraps are being planned for new construction projects.

Staff, contractors, and students are required to wear ID badges; the badges issued to staff and contractors are equipped with swipe technology to provide access to newer buildings. Visitor badges are issued for all visitors. The district is piloting the use of fingerprints for access control at one of its “open campus” high schools that has multiple buildings.

11.5.2.3 Alarms and Sensors

The district employs a number of alarms and sensors. For example, motion sensors, door position and window position alarms, and tamper alarms are all in use. Photo-beam detectors are installed on the roofs of schools in the district to monitor the school’s perimeter. Duress alarms are installed in the offices at each school. In addition, each security officer has a duress pendant, and eventually every classroom will have one. School employees who have domestic issues at home also can check out duress pendants. These alarms and sensors are tied into the burglar alarm system.

Each classroom has a speaker/call box intercom. Using the intercom, the staff in the front office can listen in on any classroom. There are also after-hours call boxes on the outside of the schools.

A lightning detection system in use across the district detects lightning strikes within 10 miles. Upon its activation, outdoor activities must cease and students must be brought indoors.

11.5.2.4 Communications

Every classroom has a 400-MHz analog radio that uses a local area network. There is also a police scanner and 800-MHz radio in every school’s front office that enables communication with local law enforcement. The “School SAFE Communications” system provides interoperability between analog radios and digital police radios. Each elementary school has two Alphones®.

The district provides an annual stipend for administrators and other key staff to have a cell phone. In addition, there are VoIP telephones in every classroom plus a landline telephone in every main office that serves as a backup means of communications. Intercoms and the PA systems are integrated into PSIM. Security personnel can use the PA system to broadcast to people after hours to, for example, prevent or stop vandalism.

An IP-based emergency notification system is used; however, to receive notification, users must enroll. In the event of a weather incident or lockdown situation, the district can send mass text and email messages; a campus management system is used for mass telephone communications. Digital signs inside and outside the school buildings are capable of displaying information required during an emergency.

Every school’s emergency “go box” contains a bullhorn.

11.5.2.5 Lighting

All schools are partially lit at night, both interior and exterior, using safety lighting. Motion sensors activate some lights. Unlike stadiums, only some practice fields have lighting; neither practice fields or stadiums are not lit when not in use.

11.5.2.6 Software

The district has acquired and routinely uses a number of electronic tools in its safety operations. While a contractor is hired to conduct security risk assessments on a periodic basis, the district prides itself on its internally developed situational awareness software. School psychologists in the district use MOSAIC^{11,12}, a violence prediction software that uses metrics and statistics to assess whether a student is a high, medium, or low threat.

The district uses a visitor management system that checks a visitor's identity against the sex offender registry as well as whether the visitor has a court filing against him or her.

To provide a means for students, staff, and others to alert the district about potential threats, two systems are in place. A state-mandated system allows users to call, text, or fill out an online form, whereas the local system provides a telephone number on the district's web site. Another means of learning about potential threats to the school, students, or staff is addressed by contracting with a company that provides keyword social media monitoring.

PSIM software has been discussed at length in Subsection 11.5.2.1.

11.5.2.7 Surveillance

Standard video cameras are extensively used for surveillance in the district. While many cameras are analog, as budget permits, the district is migrating to the exclusive use of digital cameras. One pilot study was conducted with IR cameras; however the district determined the cost was greater than the benefit. Some newer pan-tilt-zoom cameras incorporate motion-sensing capability wherein they automatically slew to the location where the motion occurred. Although only rudimentary video analytics capability is currently deployed, this is an area the district would like to expand. The bus fleet is equipped with GPS vehicle tracking and with cameras.

11.5.2.8 Weapons Detection

The district does not have technologies specifically designed to detect weapons, outside of a small number of handheld wand metal detectors.

11.5.2.9 Cyber Security

Every student has a school Gmail account that is monitored for keywords and reputation; a contractor is responsible for the monitoring. Standard firewalls and encryption are employed to protect the district's confidential and business information from accidental or intentional disclosure.

¹¹ <https://www.mosaicmethod.com/>

¹² <https://www.ncjrs.gov/pdffiles1/nij/grants/209731.pdf>

11.5.3 INTEGRATION

The PSIM system is the backbone of the district's efforts to integrate security technologies. This system is discussed in Subsection 11.5.2.1.

11.5.4 CHALLENGES AND CONCERNS

Communications generally are a challenge for the district. Over the coming months, the current mass notification system will be upgraded from a system focused on fire systems alone to one that covers eight kinds of emergencies. Because of the potential impact to the children, it is critical that the message verbiage is correct, and the district continues to work hard at this. To conform to best practices, the district has adopted the NIMS and each school has an ICS team in place. To ensure communication systems and pathways and all-hazard plans are practical and useful, the district conducts multiple tabletop exercises each year that focus on the most frequent type of emergency, like weather hazards, and less likely incidents such as active-shooter incidents. In addition, the district shares lessons learned. PSIM is especially important in this regard, as it has the capability to replay incidents or emergencies to facilitate after-action reporting and lessons learned.

11.5.5 SCHOOL SAFETY TECHNOLOGY LIST

Table 11-9 presents the school safety technologies in District 3.

Table 11-9 School Safety Technologies in Use in District 3

School Safety Technology	In Use	Comments
Access Control – Physical Barriers		
Standard door locks (lock and key); deadbolt	Yes	Older structures use standard door locks with keys; newer structures either do not have a key or have only one key for exterior doors. Interior doors do not use key locks, but they have pushbutton panic locks inside the door.
Standard window locks (latches)	Yes	
Combination locks	Yes	Used for gates and fences.
Padlocks	Yes	Used for shut off valves.
Electronic locks (remotely operated)	Yes	
Perimeter fencing	Yes	Implemented in a way that avoids the appearance of a prison.
Security or safety personnel	Yes	
Guarded entry gates	No	Some with electronic access.
Anti-ram vehicle barriers	Yes	Decorative trees and planters provide physical barriers.
Bullet-resistant glass; window films	Yes	Window laminates used on new construction projects.
One-way doors	Yes	
Turnstiles	No	
Lockdown systems	Yes	Integrated into PSIM system; capability to activate from security office and duress pendants worn by school employees.
Mantraps	No	Desire for this capability in new construction projects.

Table 11-9 School Safety Technologies in Use in District 3 (Continued)

School Safety Technology	In Use	Comments
Access Control – Means of Identification		
Swipe cards (magnetic or RFID)	Yes	Issued to all staff and contractors.
Temporary ID or visitor badges	Yes	
Staff ID cards	Yes	
Student ID cards	Yes	Worn (ID is not assured); students tend to lose them. Also used for after-school functions.
Access Control – Biometric Readers		
Fingerprint or handprint scanners and readers	Yes	Pilot program at one high school. Fingerprints being used for access control.
Iris scanners and readers	No	
Voice recognition	No	Although an option in software and mobile device platforms, capability is not being used.
Facial recognition	Yes	Part of video analytics package accompanying surveillance cameras; used forensically.
Alarms and Sensors – Intrusion and Access Alarms		
PIR motion sensors	Yes	Integrated with some cameras.
Photo and laser sensors	Yes	On school grounds perimeter; also in bus lots and on roofs.
Open door or window sensors	Yes	Current system; needs improvement.
Millimeter wave motion sensors	No	
Tamper alarms	Yes	Hard-wired or wireless installation.
Alarms and Sensors – Distress Alarms		
Distress and duress alarms or panic buttons	Yes	School employees with domestic issues at home can check out duress pendants. Every security officer has a duress pendant; eventually every classroom will also have one. Tied into the burglar alarm system.
Emergency call boxes	Yes	Speaker and call box intercom in every classroom; front office can listen in on any classroom. Each elementary school has two Alphones®. After-hours call boxes outside schools.
Alarms and Sensors – Special and Environmental Alarms		
Radiological or nuclear	No	Lightning detection system across the district that detects lightning strikes within 10 miles. Outdoor activities cease and students brought indoors.
Chemical or biological	No	
Communications – Two-way Communications		
Handheld and vehicle-mounted radios or base stations	Yes	800-MHz radios in every school office; 400-MHz radios in every classroom. “SchoolSAFE Communications” system provides interoperability between analog school radios and digital law enforcement radios.
Police scanners	Yes	In every school’s front office.
Cellular telephones (including text messaging)	Yes	District provides stipend for administrators and key staff for a cell telephone.

Table 11-9 School Safety Technologies in Use in District 3 (Continued)

School Safety Technology	In Use	Comments
Landline telephones	Yes	VoIP telephones in every classroom; backup landline in every main office.
Intercoms or PA system	Yes	Integrated into PSIM system; capability to broadcast to people after hours to, for example, prevent or interrupt vandalism.
Communications – One-way Communications		
Emergency notification system	Yes	IP-based; must enroll.
Mass telephone communication system	Yes	Campus management system.
Instant mass messaging system (text)	Yes	Used for weather emergencies, lockdown.
Automated email system	Yes	
Bullhorns	Yes	In every school's emergency "go box."
Digital signs or billboards	Yes	Interior and exterior deployment; can be used in emergencies.
Datacasting system	No	
Lighting		
Indoor lights	Yes	
Outdoor lights	Yes	Combination of scheduled lights and motion detectors.
Stadium lights	Yes	
Software		
Tip line	Yes	Two systems; one state-mandated and one local product.
Risk assessment or management software	Yes	Contracted service.
Situational awareness software	Yes	District-developed tool.
Security planning software	Yes	Use online assessment tool.
Violence prediction software	Yes	MOSAIC system leverages statistics and metrics; assesses threat.
PSIM system	Yes	
Visitor database check software	Yes	Checks sex offender registry and court filings.
Health or mental health information sharing software	Yes	Share information, though not electronically.
Social media monitoring application	Yes	Contracted keyword monitoring service; prevented a suicide in district.
Text monitoring application	No	Privacy concerns about texts.
Surveillance		
Standard video cameras	Yes	Migrating from analog to digital.
IR cameras	Yes	Have some low-light cameras; conducting pilot study using an IR camera.
Body-worn cameras	No	
Smart camera or video analytics	Yes	Basic capabilities; desire for additional capabilities.

Table 11-9 School Safety Technologies in Use in District 3 (Continued)

School Safety Technology	In Use	Comments
Gunshot location system	No	
GPS personnel tracking	No	
GPS vehicle tracking	Yes	Buses also equipped with cameras.
Weapons Detection		
Walk-through metal detectors	No	
Handheld (wand) metal detectors	Yes	A few in operation
Radar or millimeter wave weapons detection systems	No	
X-ray scanner	No	
Other Technology Systems		
Bullet-resistant white boards	No	
Pepper spray dispensers	No	
Canines	No	Local law enforcement canines are used for drug and weapons detection; searches randomly scheduled.
Safes	Yes	Used to secure contraband in security offices.
Drones	No	
Cyber and Computer Systems		
Computer systems protection	Yes	
Emails (automated email services or messaging)	Yes	Contracted service to monitor keywords and reputation; every student has Gmail account.
Anti-virus software	Yes	
Encryption software	Yes	Students challenge passwords.

11.6 CASE STUDY DISTRICT FOUR

11.6.1 DISTRICT DESCRIPTION

The study team interviewed a representative from the U.S. Department of Interior's Bureau of Indian Education (BIE). Because tribes are autonomous, no one safety specialist oversees all of the tribally operated schools, therefore the team interviewed the School Safety Specialist for the schools operated by the BIE. He has 6 years of experience in this position and more than 30 years of experience in the school environment. This case study was conducted via telephone interview.

The BIE oversees about 50,000 students in 183 schools across 23 states. Of these, 54 are Federally operated (i.e., BIE-operated schools) and 129 are tribally controlled.¹³ Federal funding comes from the Department of the Interior and the Department of Education. Of the 183 schools, 66 are boarding schools for the school week (Monday through Friday). These boarding schools are necessary because of the long commuting distances in rural areas; they are popular with the students and their families, even for very young children. There are also 300 students who attend four Off-Reservation Boarding schools; they are operated 7 days a week. It should be noted that although 50,000 students from K-12 attend the

¹³ <http://www.bie.edu/Schools/index.htm>. Retrieved 18 January 2016.

BIE schools, they represent only 10% of the Native-American student population. The other 90% attend the local public schools where they live. The tribally operated schools are grant schools that have a large degree of self-determination, although all follow state laws. The largest example of this is the schools of the Navajo nation.

For school year 2012–13, the BIE reported an average daily attendance rate of 91.4% for K-8 and 84.4% for high schools and a graduation rate of 59.8%.¹⁴ Demographic information specific to BIE schools was not identified.

In response to concerns about consistently lower performance by BIE students compared to all public school students, the U.S. Government Accountability Office (GAO) reviewed the most recent available expenditure data covering the 2009–10 school year and compared BIE school funding and expenditures with those of public schools. It found that the average per pupil expenditures for BIE-operated schools—the only BIE schools for which detailed expenditure data are available—were about 56% higher than for public schools nationally in school year 2009–10, the most recent year for which data were available at the time of GAO’s review. Several factors may help explain the higher per pupil expenditures at BIE-operated schools, such as their student demographics, remote location, and small enrollment (Reference 364).

Although security budgets are left up to individual schools to determine, the funding at the Federal level comes directly from the BIE. Previously, three safety personnel were funded at BIE, but following a restructuring there is now only one person. The BIE participates in the Safe and Secure Schools Grant and receives about \$3.9 million per year that goes to about 12 schools per year that have been earmarked for security upgrades. The fairly secure funding stream allows different schools to be selected.

BIE schools are required to have an emergency management plan for facilities that is updated annually per policy. There is a 2009 template on the website for schools to access and use. Technologies are not addressed in the plan other than cell phones, radios, and intercoms.

Students and staff conduct monthly evacuation drills, such as fire drills. There is one active-shooter lockdown drill per year, but it is not required. Four terms are used: evacuation, reverse evacuation (everyone on the playground comes inside), lockdown, and shelter in place. In terms of metrics or effectiveness of drills, a report is sent to the safety specialist, who must keep records on hand.

At the Federal level, there are many organizational relationships with professional societies and other Federal agencies. Examples include the Department of the Interior Emergency Management, Department of Homeland Security, Bureau of Indian Affairs, Federal Bureau of Investigation, and Federal Emergency Management Agency. At the local level, there is engagement with local law enforcement as well as the Tribal Assistant Group Coordinator.

11.6.2 SCHOOL SAFETY TECHNOLOGIES IN USE

11.6.2.1 Featured Technology

There was no featured technology targeted for the BIE case study interview. Rather, all security technologies were discussed.

¹⁴ Bureau-Wide Annual Report. <http://www.bie.edu/cs/groups/xbie/documents/text/idc1-026197.pdf>

11.6.2.2 Access Control

A variety of access control technology is used at BIE schools. All classrooms have locks; teachers have keys for their classrooms. Administrators at the schools decide whether classroom doors must be locked while students are present. A few schools use a system that will lock all doors with a single button press. Most, however, require teachers to walk into the hallway and use a key to lock their classroom door. Combination locks are used primarily on lockers, although there is a desire to use combination cypher locks on doors. For schools less than 5 years old, some electronic locks are being installed on exterior doors; 5% to 10% of schools require visitors to be buzzed in prior to admittance.

Although the Office of the Inspector General requires perimeter fencing, some schools have minimal fencing, allowing an individual to walk in undetected. Some gates are open all the time, but this is being addressed. In a handful of schools, the Federal Bureau of Investigation provides staff as SROs. In addition, there are a few contracted security guards and guarded entry gates at Off-Reservation Boarding schools.

The staff and faculty have ID cards, but they do not provide access control. Visitor badges are worn and must be visible. Some schools also require students to wear ID cards.

11.6.2.3 Alarms

Alarms intended to secure individual schools are not prevalent. PIR motion detectors are used in conjunction with outdoor lighting. In addition, when a motion detector is used inside a building, it is integrated into the school alarm system. Less than 50% of classrooms have distress alarms for use during an emergency.

11.6.2.4 Communications

A number of one-way and two-way communications devices are used in BIE schools. Handheld radios are used by the security staff who patrol the grounds and by staff who are located in portable classrooms. Weather-alert radios are widely used. Personal cell phones are used. Although the BIE provides cell phones to some individuals, some schools have no reception. Therefore, landline telephone systems are installed in every office, but not always in every classroom. A few remote schools have satellite phones; more would be beneficial. Although portable classrooms may not have them, intercoms and PA systems are used and are particularly effective in communicating outside the school building.

The BIE has direct call emergency notification systems that can call parents in the event of an emergency, but fewer than 10% of schools have them. Students, parents, teachers, or others can use WeTip,¹⁵ a national service that provides an anonymous hotline and an online digital presence, to report crimes to the BIE. Almost half of the schools have digital signs in the cafeteria that can be used to disseminate emergency messages.

11.6.2.5 Lighting

The BIE uses indoor and outdoor security lighting at its schools. More lighting is desired, especially for the dormitories.

¹⁵ <http://wetip.com>, retrieved 18 January 2016.

11.6.2.6 Software

The BIE currently uses few electronic tools in its safety operations. An electronic template is available to help conduct risk assessment and risk management. Situational awareness for weather alerts is maintained manually by consulting the Department of Interior Watch Office. Send Word Now® is an important electronic communication, collaboration, and notification tool used in response to ongoing emergency planning.

The limited social media monitoring by authorities is based on tips from staff, students, or parents about something they themselves learned on social media. There is a manual recordkeeping system for tracking drug offences, fights, and bullying.

11.6.2.7 Surveillance

The BIE has some limited surveillance capability. Almost all schools have standard video cameras, but may leave some areas uncovered and the video feed is simply recorded rather than monitored. Some new buildings have IR cameras with motion-following capability. Lastly, some buses have GPS tracking installed.

11.6.2.8 Weapons Detection

Although some schools own handheld metal detectors, they are not being used currently in BIE schools.

11.6.2.9 Other Technology Systems

Local county law enforcement canines are used for drug searches. Special education records are stored in fireproof cabinets.

11.6.2.10 Cyber Security

The schools use firewalls and anti-virus software.

11.6.3 IMPLEMENTATION ASPECTS OF TECHNOLOGY

Recently, an increasing number of surveillance cameras have been installed at some schools. The cameras seem to be effective as deterrents and are used as investigative tools. There also seems to be an increase in the willingness of staff to challenge strangers. Many schools have large acreage, and they are trying to decrease acreage to more effectively manage their area of responsibility. Lastly, there appears to be an increase in the number of parents checking in with the schools.

Table 11-10 presents the implementation aspects of using technology at BIE schools.

Table 11-10 Implementation Aspects for Technology at BIE Schools

Implementation Aspect	Comments
Installation	BIE has to hire contractors when installing technology because its schools are Federal facilities. This causes long delays to get technology installed, potentially affecting school safety.
Training	There are no concerns with training on safety technologies.
Maintenance	The school budget accommodates maintenance of security technology.
Consumables	Wiring for the fire alarm system has to be replaced frequently because it is easily damaged in freezing conditions.
Policies	The BIE allows audio recording on surveillance cameras. The administrators decide who can see the video. The staff has not reported issues with audio being recorded.
Personnel and culture of security	All staff are responsible for challenging someone who does not belong in the hallway or grounds. The staff receives training on this, and that has become the expectation. Before training, a “test” intruder would typically be on the grounds for 90 minutes before being challenged. Now that time has decreased to 10 minutes.

11.6.4 INTEGRATION

There is very little integration of technology noted in the tribal schools. There is limited integration of alarms with locks and alarms with motion detectors.

11.6.5 CHALLENGES AND CONCERNS

The biggest deterrent to violence is that schools are small and the staff know their students. Staff can make a difference by intervening before violence happens.

One major concern is the remote location of many schools. For these schools, it would take the nearest first responders 30 to 60 minutes to arrive at the school by car. Despite this, significant gains have been made in relationship building, particularly between schools, local law enforcement, and hospitals. Because the fire department and law enforcement often use school buildings for response practice and to gain familiarity with the building, a relationship exists between schools and first responders before an incident happens.

Another concern has been related to access to schools and school property due to leaving doors propped open to allow smoke breaks, to ventilate cooking heat and while waiting for deliveries. Moreover, the disrepair of some fences allows community members open access school grounds. However, attitudes over the past six to seven years have changed, resulting in an increase in safety focus at the schools. The staff therefore has become more aware of different response scenarios.

11.6.6 SCHOOL SAFETY TECHNOLOGIES IN USE

Table 11-11 presents the school safety technologies in use at BIE schools.

Table 11-11 School Safety Technologies at BIE Schools

School Safety Technology	In Use	Comments
Access Control – Physical Barriers		
Standard door locks (lock and key); deadbolt	Yes	Keys for each classroom.
Standard window locks (latches)	Yes	
Combination locks	Yes	On lockers and some exterior doors; combination cypher locks desired.
Padlocks	Yes	On perimeter fencing and student lockers.
Electronic locks (remotely operated)	Yes	On newer buildings. Emergency exits use magnetic locks; they will unlock if the alarm activates. No ability to perform automated lockdowns.
Perimeter fencing	Yes	Required by the inspector general. Some are in disrepair; some gates are open all the time (being corrected).
Security or safety personnel	Yes	A few contract security guards at boarding schools.
Guarded entry gates	Yes	At boarding schools plus additional one or two schools.
Anti-ram vehicle barriers	No	
Bullet-resistant glass; window films	No	No bullet-resistant glass or window film; some reflective window film.
One-way doors	Yes	Used for access-restricted doors.
Turnstiles	No	Discussions about using in conjunction with fencing.
Lockdown systems	Yes	Majority is basic; in a few schools a single button will lock all doors.
Mantraps	Yes	5% to 10% of schools use them; administrator decision about whether to keep the doors locked inside the building.
Access Control – Means of Identification		
Swipe cards (magnetic or RFID)	No	Not for access.
Temporary ID or visitor badges	Yes	
Staff ID cards	Yes	Must be visible.
Student ID cards	Yes	Some schools require students to wear ID cards.
Access Control – Biometric Readers		
Fingerprint or handprint scanners and readers	No	Employees must pass background check with fingerprint; are not used for building access.
Iris scanners and readers	No	
Voice recognition	No	
Facial recognition	No	

Table 11-11 School Safety Technologies at BIE Schools (Continued)

School Safety Technology	In Use	Comments
Alarms and Sensors – Intrusion and Access Alarms		
PIR motion sensors	Yes	Use in conjunction with outdoor security lighting at night: also used inside buildings.
Photo and laser sensors	No	
Open door or window sensors	No	
Millimeter wave motion sensors	No	
Tamper alarms	No	
Alarms and Sensors – Distress Alarms		
Distress and duress alarms or panic buttons	Yes	Less than 50% of classrooms.
Emergency call boxes	No	
Alarms and Sensors – Special and Environmental Alarms		
Radiological or nuclear	No	
Chemical or biological	No	
Communications – Two-way Communications		
Handheld and vehicle-mounted radios or base stations	Yes	Used by security staff who patrol the grounds and by staff located in portable classrooms.
Police scanners	No	Weather-alert radios used.
Cellular telephones (including text messaging)	Yes	Personal cell phones used; some provided by the schools. Reception unavailable in some locations.
Landline telephones	Yes	Not every classroom; a few schools have satellite phones (desire for more).
Intercoms or PA system	Yes	Portable classrooms may not have them; PA systems on exterior grounds.
Communications – One-way Communications		
Emergency notification system	Yes	Less than 10% of schools have direct call systems to notify parents in the event of an emergency.
Mass telephone communication system	No	There is a desire for this capability.
Instant mass messaging system (text)	No	
Automated email system	No	
Bullhorns	Yes	
Digital signs or billboards	Yes	Nearly half the schools have them in the cafeteria.
Datacasting system	No	
Lighting		
Indoor lights	Yes	
Outdoor lights	Yes	Desire for additional lights around dormitories.
Stadium lights	Yes	

Table 11-11 School Safety Technologies at BIE Schools (Continued)

School Safety Technology	In Use	Comments
Software		
Tip line	Yes	Capability exists at the national level, not at the school level.
Risk assessment or management software	No	Template available but not software.
Situational awareness software	Yes	A watch office that sends out weather alerts, etc.
Security planning software	No	
Violence prediction software	No	Recordkeeping system for drug offences, fights, bullying, etc.
PSIM system	No	
Visitor database check software	No	Manually check visitor ID.
Health or mental health information sharing software	No	
Social media monitoring application	No	Staff, student, family may refer something learned on social media.
Text monitoring application	No	
Surveillance		
Standard video cameras	Yes	Coverage usually insufficient; feed is not monitored, just recorded.
IR cameras	Yes	Follow motion; deployed in new buildings only.
Body-worn cameras	No	
Smart camera or video analytics	No	
Gunshot location system	No	
GPS personnel tracking	No	
GPS vehicle tracking	Yes	On some buses.
Weapons Detection		
Walk-through metal detectors	No	
Handheld (wand) metal detectors	Yes	Some schools have; not used.
Radar or millimeter wave weapons detection systems	No	
X-ray scanner	No	
Other Technology Systems		
Bullet-resistant white boards	No	
Pepper spray dispensers	No	
Canines	No	Local law enforcement canines for drugs.
Safes	Yes	Fireproof cabinets used for special education records.
Drones	No	

Table 11-11 School Safety Technologies at BIE Schools (Continued)

School Safety Technology	In Use	Comments
Cyber and Computer Systems		
Computer systems protection	Yes	Firewalls are used.
Emails (automated email services or messaging)	No	
Anti-virus software	Yes	
Encryption software	No	

11.7 CONCLUSION

The authors synthesized the information collected during interviews with four school districts into case studies to provide concrete examples of the school safety technologies deployed in actual school environments. This snapshot in time allows readers to gain an understanding of the current technology in use, its implementation, and considerations affecting implementation. By providing an overview of technologies and a profile of the school district, the case studies provide context for the use of school safety technologies in real-world settings.

All four districts that participated as case studies are concerned about school safety, and all use technology in varying degrees to make their schools safer. However, they all stressed that technology cannot be used in isolation. There is hard work—from strategic and emergency planning to relationship building to drills—that must accompany the deployment of any technology. Each district provided anecdotes suggesting technology made their schools districts safer, but none could point to data or metrics that demonstrated a causal relationship between the deployment of safety technology and prevention or reduction of acts of criminal violence. Nonetheless, each district had a “wish list” of additional technology measures to implement.

Because of the small sample size, it is inappropriate to generalize the case study data to a larger population. Nevertheless, participants all mentioned increasing acceptance and commitment in the school community of students, parents, teachers, administrators, and staff to safer, more secure schools. For example, commitment to ensuring exterior doors remain closed during school hours was a point of emphasis. A desire for increased understanding, or situational awareness, of the security in the districts, mainly through technology, was expressed. Communications were consistently highlighted as very important. Multiple districts were also interested in Tip lines and basic locks indicating that basic technologies are recognized as a valuable addition to more high-tech forms of security technology.

Available resources, internal commitment, and tradeoffs between security and school operations will occur. However, based on the information obtained from the case studies, reliance on technology to make schools safer will continue.

This page intentionally left blank.

Chapter 12. LEGAL REVIEW

Julia A. Wolfson, MPP; Anna L. Davis, JD MPH; and Stephen P. Teret, JD MPH

12.1 INTRODUCTION

Technology is one of the tools that can be used to make schools safer and more secure; law is another.

Laws, in all their forms, have a broad reach. They can compel or prohibit specified behaviors, they can require certain designs of the built environment, and, more germane to this report, they can mandate or limit the use of technologies in schools for the protection of those within them. Throughout this chapter, the authors provide examples of how the law enables schools to use technology to ensure the safety of their staff and students.

There are several sources of the law. The Constitution of the United States and individual state constitutions provide broad principles of law. These principles are given clearer application to everyday life when legislative bodies make statutory law, governmental agencies promulgate regulations, and courts both judge the constitutionality and validity of statutes and regulations and make what is called common law when the courts decide on the outcomes of certain types of lawsuits.

Lawmaking takes place at the Federal, state, local, and tribal government levels. There is a hierarchy of laws in that Federal law sometimes will preempt state and local laws, and state law can also preempt local law. By “preempt,” lawyers mean that, for example, a state or local law may be considered invalid by the courts if a Federal law either expressly or impliedly fully occupied that area of lawmaking. Also, regulations in general will only be deemed valid if there was statutory authority given by a legislature to a governmental agency to promulgate regulations on a given topic.

The work described herein looked mainly at statutory and regulatory law at the Federal and state levels to determine whether the law enables or prohibits the use of specific technologies that are designed to protect students, faculty, and staff in K-12 schools.

The primary objective of this chapter is to provide an overview of the statutory and regulatory law at the Federal and state levels that guide (by requiring, permitting or restricting) the use of technology in preventing or mitigating school violence. Several local-level regulations in localities identified through a search of news media coverage of school safety and technology are also profiled. The secondary aim of this chapter is to examine the nature of discourse regarding school safety and technology in major newspapers in the United States.

Section 12.2 first describes the methodology used to identify and code Federal and state laws authorizing the use of technology for school safety and the analysis of both legal and news media samples. Subsection 12.2.2 presents the results of the analysis of the Federal and state statutes and regulations and discusses some local-level examples. Lastly, Subsection 12.2.3 discusses the results of the news media analysis. Also presented are the implications of the authors’ findings (Section 12.3), the limitations of their analysis (Section 12.4), and some concluding thoughts (Section 12.5).

12.2 METHODOLOGY

12.2.1 DATA COLLECTION

12.2.1.1 Federal and State Statutes and Regulations

The research team conducted a survey of current laws related to school safety, specifically searching for laws authorizing the use of technology to prevent or mitigate criminal acts of violence in K-12 schools, both public and private. Laws regulating the use of firearms and less-than-lethal or compliance weapons in schools were excluded from the survey, as were any laws or policies that focused primarily on bullying prevention programs or drug and alcohol use. Safety-related technology, for purposes of this report, is defined as any device or mechanism applied or installed in schools to prevent, mitigate, or deter criminal acts of violence that may occur in the school environment. Examples of such technologies include, but are not limited to, surveillance cameras and communication systems, alarms, door locks and other entry control systems, weapons detection devices, emergency alert systems, protective glass, interior and exterior lighting systems, social media monitoring, and global positioning systems.

Using the Westlaw and LexisNexis electronic legal databases, which are commonly used in legal research, the team conducted a survey of Federal and state statutes and administrative regulations in all 50 states, the District of Columbia, and the territorial jurisdictions of Guam, Puerto Rico, the U.S. Virgin Islands, and the Northern Mariana Islands. Tribal jurisdictions were also included. Research was limited to law that specifically addressed school safety and the application of technology to enhance the security of the school environment.

The initial searches were deliberately over-inclusive so as to capture the broadest range of relevant provisions contained in law. The research team determined the final search terms through an iterative process and by reviewing the content of preliminary search results. They used numerous iterations of varied search terms to identify relevant provisions of current legal codes and administrative regulations. Final search terms included the following: *school, security, safety, emergency or crisis plan, technology, prevention, violence, surveillance, communication, access, detect, and drill*. To maximize results, the team applied the root expander (!) to retrieve all variations of key words. For example, “prevent!” returned *prevent, prevented, preventing, and prevention*.

The initial searches returned a total of 609 statutes and 370 regulations. The title and description of each document were reviewed to determine relevancy. Statutes and regulations that were not substantively related to school safety and technology were excluded. Relevant results were collected and downloaded into files for analysis and coding. The team employed snowball sampling to pursue and collect additional sources that were not retrieved via the original search terms. For example, if upon review of a particular statute, another statute or regulation was cited, the referenced text was retrieved to determine its relevancy for inclusion in the final data set.

The final search yielded 119 Federal and state statutes and regulations. After a full text review, six were excluded because they were not substantively related to school safety and another four were excluded because they were not focused on violence prevention (i.e., they were focused on drugs or bullying). The final analytic sample included 109 sources of which five were Federal statutes, 85 were state statutes, and 19 were state regulations.

12.2.1.2 Local Laws and Regulations

There is no one central electronic legal database to search for local laws and regulations; therefore, the research team used newspaper coverage as its search starting point. Through the analysis of the newspaper sample (described in more detail next), the team identified 25 localities (school districts, cities, or counties) in which schools had implemented or considered implementing school safety technologies of interest. The team conducted a targeted search of policies and guidelines used by the local school boards within those localities by visiting the website of the school or local board of education. The search of these online resources was prompted solely by cues derived from local news coverage and yielded results that are available to the general public. Because this search was neither a systematic review of local laws nor a search using electronic legal databases, the results are not exhaustive. There are local- or district-level policies and procedures that may exist in other localities that were not identified through this search and are therefore not included in this report. As will be discussed further, the team obtained local regulations and district policy documents regarding school safety and violence prevention procedures from 21 school districts out of the initial sample of 25 localities.

12.2.1.3 Newspaper Coverage

The research team used ProQuest Newsstand, a database commonly used in research about media coverage, to search coverage of school safety and technology in 10 major newspapers in the United States. News sources included four of the highest circulation national newspapers in the United States (*Wall Street Journal*, *New York Times*, *USA Today*, and *The Washington Post*), and one of the highest circulation newspapers in each of the U.S. census regions, including the Northeast (*New York Daily News*), South (*Tampa Bay Times*), Midwest (*Chicago Tribune*), and West (*Los Angeles Times*). Also included were news stories from two local papers (*The Denver Post* and *The Baltimore Sun*). To focus on currently available technologies and recent public discourse, the team limited the search to articles published between 1 January 2010 and 20 June 2015 and used the following search terms: ("school safety") AND (technology OR access OR surveillance OR alarm OR communication OR cyber OR detect). This search yielded an initial sample of 493 articles, of which 273 were excluded based on a review of titles and abstracts because they were not substantively related to school safety or technology. Of the 220 remaining articles, 52 were excluded upon review of the full text because they were either not focused on school safety or were focused on non-violence school safety measures (i.e., drugs or bullying), resulting in a final analytic sample of 168 articles.

12.2.2 ANALYSIS

12.2.2.1 Federal and State Statutes and Regulations

The team developed a coding document to analyze the content of the legal sample (statutes and regulations) regarding school safety and technology. This document consisted of 40 items and focused on whether technology categories or specific technologies were mentioned in the statute or regulation. For example, "Does the statute mention access control technology? [Yes/No]." If mentioned, whether the law in question required the technology, limited the use of the specific technology, or prohibited the use of the technology was coded.

The full sample of statutes and regulations was coded by one member of the research team, and the full news media sample was coded by another member. Throughout the coding process the full research team met frequently to discuss coding and to adjudicate any instances where the application of a code

was unclear. Local-level laws were treated as case studies and were qualitatively analyzed by members of the research team.

The research team stratified the legal sample by the type of document [Federal statute (N = 5), state statute (N = 85), or state regulation (N = 19)] and examined each type of law separately. First, the team created binary indicators for each document measuring whether technology was mentioned at all, and if so, whether the document required specific technologies for school safety or whether the document placed any limit on the use of technology for school safety. For example, if a document mentioned a specific technology (e.g., locks, metal detectors, alarms) it was coded as “Yes” (having mentioned technology), and if it discussed school safety without mentioning any specific technology it was coded as “No.”

Next, the team consolidated the data at the state level for the 49 jurisdictions with at least one relevant statute. The team created binary measures for the following outcomes:

- Whether or not any statute in the state mentioned technology
- Whether or not funding for technology was specified
- Whether or not an implementation deadline was specified
- Whether technology for school buses was specified
- Whether technology was required, and if so, whether the funding or implementation deadline was specified
- Whether any statute in the state placed limits on technology

This process was replicated for the Federal statutes and the 17 states with at least one relevant regulation. For example, in a jurisdiction with four statutes covering school safety, if one of them mentioned technology but the other three did not, that jurisdiction was coded as mentioning technology. The team then calculated the percentage of jurisdictions with statutes and regulations in which technology in general was mentioned (as opposed to school safety with no mention of technology); whether specific technologies were mentioned, and if so, whether technologies were required or limited; whether technology in school buses was mentioned; and whether implementation deadlines or funding mechanisms were specified.

Lastly, the team pooled the sample of Federal statutes, state statutes, and state regulations and examined the number of sources in which each individual technology was mentioned.

12.2.2.2 Newspaper Coverage

The coding document for the news media sample consisted of 34 items and focused on whether broad categories of technology were mentioned (e.g., access control, surveillance or weapons detection) and if so, whether positive and/or negative opinions of the technology were expressed. In addition, the team coded news stories for overall assessments of technology in schools, reasons technology is needed, and a variety of considerations regarding the use of technology for school safety.

For the newspaper sample, the research team calculated the raw number and percentage of articles in which technology was mentioned (as opposed to school safety with no mention of technology), and if technology was mentioned, whether positive opinions only, negative opinions only, both positive and negative opinions, or no opinion was expressed. More general supporting and opposing messages contained within news stories about school safety were also examined. All analyses were conducted using the statistical analysis software Stata, version 13 (Stata-Corp LP, College Station, Texas).

12.2.3 RESULTS

The data collection yielded many examples of statutory and regulatory law dealing with technology for school safety. Overall results are presented in the tables and the subsection narrative places these results in context through exemplary quotations and legal analysis. Table 12-1 briefly describes the 109 individual Federal and state statutes and state administrative regulations, their official citations, and whether or not they mention, require, or limit technology for the purposes of ensuring school safety.

Figure 12-1 displays the frequency with which individual technologies are mentioned in Federal and state laws (both statutes and regulations). Among the 109 laws included in this sample, metal detectors were referenced most frequently (in 9 laws). Locks and cameras were the second most cited technologies (six times each) in state laws.

12.2.3.1 Federal Statutes

Of the five Federal statutes identified, three mentioned technology, and of those, two require the use of technology.¹ Any local educational agency (LEA) that receives Federal money under the Safe Schools program “shall use grant funds” for a number of activities, including but not limited to the acquisition and purchase of metal detectors.² Similarly, violence prevention activities under the Safe and Drug-Free Schools and Communities Act include “metal detectors, electronic locks, surveillance cameras, or other related equipment and technologies.”³ The Act limits the use of technology for school safety in that any LEA that receives grant monies under that program must conduct weapons inspections in a manner “consistent with the guarantees of the Fourth Amendment to the Constitution of the United States.”⁴ Courts, however, generally interpret such restrictions broadly, finding that the governmental interest of preventing crime in schools overrides students’ expectations of privacy (Reference 230). (Also see Reference 231, which discusses the steady decline in students’ Fourth Amendment rights and judicial justification of random, suspicion-less search practices in schools and noting that courts routinely uphold the use of metal detectors, random sweeps, surveillance cameras, locked gates, and law enforcement officers in schools.)

¹ 20 USC. 5965(A)(13); 20 USC. 7115(b)(2)(E)(ii)

² 20 USC. 5965(A)(13)

³ 20 USC. 7115(b)(2)(E)(ii)

⁴ Id. at 7115(b)(2)(E)(xiv)

Table 12-1 U.S. Federal and State Statutes and Regulations on School Safety

State	Citation	Mentions Technology	Requires Technology	Limits Technology	Description
Federal Statutes (N = 5)					
N/A	20 USCA §§ 5962 – 5966 (1994)	Yes	Yes	No	Authorizes awards of competitive grants to local educational agencies through the Safe Schools program; requires comprehensive school safety plans; requires acquisition and installation of metal detectors
N/A	20 U.S.C.A. § 7115 (2002)	Yes	Yes	Yes	Authorizes local educational agencies to use grant monies to acquire and install metal detectors, electronic locks, surveillance cameras or other related equipment and technologies and to develop and implement comprehensive school security plans; violence prevention activities must be consistent with the Fourth Amendment to the Constitution of the United States
N/A	20 USCA § 7137 (2002)	Yes	No	No	Establishes the School Security Technology and Resource Center at Sandia National Laboratories in Little Rock, Arkansas
N/A	20 USCA § 7138 (2002)	No	No	No	Authorizes the Secretary of Education and Attorney General jointly to establish a National Center for School and Youth Safety
N/A	6 USCA § 603 et. seq. (2007)	No	No	No	Establishes as part of Homeland Security Grants the Urban Area Security Initiative to provide grants to assist high-risk urban areas in preventing, preparing for, protecting against, and responding to acts of terrorism
State Statutes (N = 85)					
Alabama	Ala. Code 1975, § 16-1 – 44	Yes	No	No	Requires adoption of comprehensive school safety plans; allows for locked doors and exits in schools
Alaska	Alaska Stat. § 14.33.100	Yes	Yes	No	Requires development of school crisis response plan that must include a communication and lock down plan
Arizona	Ariz. Rev. Stat. § 15-154	No	No	No	Allows school districts to apply for grant to participate in school safety program
	Ariz. Rev. Stat. § 15-341	No	No	No	Authorizes school district governing board to develop an emergency response plan
Arkansas	Ark. Code Ann. § 6-15-1301 – 1303	Yes	Yes	No	Directs State Department of Education to create a Safe Schools Committee; Creates 2015 School Safety Act; requires panic button alert systems in public schools

Table 12-1 U.S. Federal and State Statutes and Regulations on School Safety (Continued)

State	Citation	Mentions Technology	Requires Technology	Limits Technology	Description
California	Cal. Ed. Code § 32228	No	No	No	Declares legislative intent that students in grades 8 through 12 have access to resources that promote school safety and violence prevention
	Cal. Ed. Code §§ 32228.1 - 32228.2	Yes	Yes	No	Establishes School Safety and Violence Prevention Act and allocates funds to school districts; allows funds to be used for “on-campus communication devices and other school infrastructure safety needs”
	Cal. Ed. Code §§ 32280 - 32282	No	No	No	Requires development of comprehensive school safety plans with strategies aimed at education and the prevention of crime and violence in schools
	Cal. Ed. Code §§ 32261 - 32262	No	No	No	Declares legislative support for public schools to develop comprehensive safety plans in coordination with local law enforcement; establishes the School/Law Enforcement Partnership
Colorado	Colo. Rev. Stat. Ann. § 22-32-109.1	Yes	No	No	Requires Board of Education to develop a National Incident Management System (NIMS)-compliant school response framework
	Colo. Rev. Stat. Ann. § 24-33.5-1213.4	No	No	No	Creates duty of emergency response personnel to coordinate the incident response framework with schools and to oversee emergency preparedness plans
Connecticut	Conn. Gen. Stat. Ann. § 10-222m	No	No	No	Requires development and implementation of school security and safety plans; establishes a school security and safety committee at each school
	Conn. Gen. Stat. Ann. § 10-222n	No	No	No	Sets forth standards for school security and safety plan
	Conn. Gen. Stat. Ann. § 10-292r	Yes	Yes	No	Establishes a School Safety Infrastructure Council; sets forth safety standards to be incorporated in school infrastructure, including reinforced entryways, ballistic glass, solid core doors, computer-controlled electronic locks, cameras and closed circuit television monitoring and “other security infrastructure improvements and devices as they become industry standards”
Delaware	14 Del. C. § 1421	Yes	Yes	Yes	Authorizes school board to establish and implement programs to use video cameras for surveillance on school property
	14 Del. C. § 4119	Yes	Yes	No	Authorizes school board of each school district to employ the use of metal detectors or other similar security devices in schools
	29 Del. C. § 8237	Yes	No	No	Creates Omnibus School Safety Act to enhance public safety in public schools through the development and maintenance of comprehensive, site-specific, NIMS-compliant safety and emergency preparedness plans
District of Columbia	DC. Code Ann. § 5-132.02	No	No	No	Establishes the Metropolitan Police Department School Safety Division; requires creation and implementation of security and emergency operations plans in DC public schools

Table 12-1 U.S. Federal and State Statutes and Regulations on School Safety (Continued)

State	Citation	Mentions Technology	Requires Technology	Limits Technology	Description
	DC. Code Ann. § 5-132.03	No	No	No	Provides for development of training curriculum for school security personnel
Florida	Fla. Stat. Ann. § 1006.07	Yes	Yes	No	Specifies duty of school board to formulate and prescribe policies and procedures for emergency drills and actual emergencies; requires policies to include the use of alarm system responses for verification of emergency drills
Georgia	Ga. Code Ann. § 20-2-1185	Yes	Yes	No	Requires public schools to prepare a school safety preparedness plan; authorizes funding requests for “video surveillance cameras, metal detectors, and other similar security devices”
Hawaii	None				
Guam	17 Guam Code Ann. § 3112.2	No	No	No	Requires education board to adopt a policy to address crimes within schools
Idaho	None				
Illinois	105 Ill. Comp. Stat. Ann. § 128/1 et seq. “School Safety Drill Act”	No	No	No	Enacts School Safety Drill Act; establishes minimum requirements and standards for school in conducting safety drills and reviewing emergency and crisis response plans
Indiana	Ind. Code Ann. § 10-21-1-2	Yes	Yes	No	Establishes secured school fund to provide matching grants to schools for the purchase of equipment and technology that will restrict access to school property or expedite notification to first responders
	Ind. Code Ann. § 5-2-10.1-1.7 et seq.	No	No	No	Defines school safety plan; mandates designation of school safety specialists in each school corporation; authorizes each county to establish a county school safety commission
Iowa	Iowa Code § 423E.6	No	No	No	Establishes a school infrastructure safety fund to provide grants to improve school safety plans
Kansas	Kan. Stat. Ann. § 72-89b03	No	No	No	Requires each board of education to make available district policies and reports concerning school safety and security
Kentucky	Ky. Rev. Stat. Ann. § 158.442	No	No	No	Authorizes establishment of Center for School Safety
	Ky. Rev. Stat. Ann. § 158.445	No	No	No	Requires local school boards to adopt a safety plan that incorporates immediate and long-term strategies to address school safety and student discipline
Louisiana	La. Rev. Stat. Ann. § 17:81	Yes	Yes	Yes	Authorizes city and parish school boards to purchase appropriate metal detection devices, to develop a plan for use and training of metal detection devices
	La. Rev. Stat. Ann § 17:3996	No	No	No	Requires charter schools to have school crisis management and response plans that comply with rules and regulations applicable to public schools

Table 12-1 U.S. Federal and State Statutes and Regulations on School Safety (Continued)

State	Citation	Mentions Technology	Requires Technology	Limits Technology	Description
	La. Rev. Stat. Ann. § 17:416.16	Yes	No	No	Defines crisis management and response plan and mandates the plan to be prepared by each public school principal jointly with local law enforcement officials, first responders, and emergency preparedness officials; plans shall require locked classroom doors
Maine	Me. Rev. Stat. Ann. tit. 20-A, § 1001	No	No	No	Requires school boards to approve a comprehensive emergency management plan
Marianas Islands	None				
Maryland	Md. Educ. Code Ann. § 7-1502	Yes	Yes	No	Establishes the Maryland Center for School Safety that shall assist school systems determine the need for surveillance and other security technology
Massachusetts	Mass. Gen. Laws Ann. ch. 70B § 14	No	No	No	Authorizes the cost of approved construction projects for upgrades and technological devices necessary for enhanced safety and security
Michigan	Mich. Comp. Laws Ann. § 380.1308	No	No	No	Mandates adoption of statewide school safety information policy identifying the types of incidents that must be reported to law enforcement agencies
	Mich. Comp. Laws Ann. § 380.1310a	No	No	No	Requires school boards to report incidents of crime occurring at school within the school district
Minnesota	Minn. Stat. § 127A.051	No	No	No	Establishes a multiagency leadership council to improve school climate and school safety
	Minn. Stat. § 127A.052	No	No	No	Establishes a school safety technical assistance center focusing on prevention, intervention, support, and recovery efforts to develop and maintain safe and supportive schools
Mississippi	Miss. Code Ann. § 37-3-83	Yes	No	No	Establishes a School Safety Grant Program offering specific preventive services including metal detectors, video surveillance cameras, communications equipment and monitoring equipment for school buildings and school buses
Missouri	Mo. Ann. Stat. § 160.660	No	No	No	Mandates inclusion of information related to violence prevention programs and resources in criteria developed for school improvement program
Montana	Mont. Code Ann. § 20-1-401	Yes	No	No	Requires adoption of a school safety plan or emergency operations plan; must address communication systems
Nebraska	Neb. Rev. Stat. Ann. § 79-2,144	No	No	No	Defines duty of state school security director to include, <i>inter alia</i> , collection of safety and security plans, recommending minimum standards for school safety, conducting security assessments, and establishing security awareness and preparedness tools and training programs
Nevada	Nev. Rev. Stat. Ann. § 392.620	No	No	No	Requires development of one plan to be used by all public schools in school district in responding to a crisis or emergency

Table 12-1 U.S. Federal and State Statutes and Regulations on School Safety (Continued)

State	Citation	Mentions Technology	Requires Technology	Limits Technology	Description
	Nev. Rev. Stat. Ann. § 392.624	No	No	No	Requires annual review and updating of plan adopted pursuant to Nev. Rev. Stat. Ann § 392.620
	Nev. Rev. Stat. Ann. § 392.640	No	No	No	Mandates detailed model plan for the management of a crisis or emergency in a public school
	Nev. Rev. Stat. Ann. § 394.1691	No	No	No	Requires private schools to conduct annual review of emergency management plan
New Hampshire	N.H. Rev. Stat. Ann. § 189.64	No	No	No	Requires every public and nonpublic school to develop a site-specific school emergency response plan based on and in conformance with NIMS
	N.H. Rev. Stat. Ann. § 193-G:6	No	No	No	Authorizes schools to implement policies promoting school safety
New Jersey	N.J. Rev. Stat. § 18A:41-1 et seq.	No	No	No	Requires monthly school security drills
	N.J. Rev. Stat. § App. A:9-86	No	No	No	Directs state domestic security agencies to develop a security drill guide and training materials on school security for dissemination to local school districts
	N.J. Rev. Stat. § App. A:9-43-7	No	No	No	Permits school districts to submit by electronic format comprehensive school safety plans to state office of emergency management
New Mexico	N.M. Stat. Ann. § 22-13-14	No	No	No	Requires emergency drills in public and private schools
New York	N.Y. Educ. Law § 2814	Yes	Yes	No	Authorizes the award of grant monies for purchase of “metal detectors, intercom and other intra-school communication devices and other devices to increase school security and safety...”
	N.Y. Educ. Law § 2801-a	Yes	Yes	No	Mandates comprehensive district-wide and building-level school safety plans that address crisis intervention and emergency response and management; requires policies related to security devices and internal and external communication systems
North Carolina	N.C. Gen. Stat. Ann. § 115C-105.33	No	No	No	Permits a school improvement team or parent organization to request that the “local board of education provide assistance in promoting or restoring safety and an orderly learning environment at a school”
	N.C. Gen. Stat. Ann. § 115C-105.49	No	No	No	Requires full system-wide school safety and school lockdown exercises every two years
North Dakota	None				
Ohio	Ohio Rev. Code. Ann. § 3313.536	No	No	No	Requires adoption of comprehensive emergency management plan
Oklahoma	Okla. Stat. Ann. tit. 70, § 5-149	No	No	No	Mandates all public schools to conduct safety drills which shall include two intruder drills as an alternative to the lockdown method
	Okla. Stat. Ann. tit. 70, § 51.2d	Yes	No	No	Creates the Oklahoma School Security Institute; authorizes use of a telephone tip line
	Okla. Stat. Ann. tit. 74 § 51.2d	Yes	No	No	Establishes the Oklahoma School Security Grant Program

Table 12-1 U.S. Federal and State Statutes and Regulations on School Safety (Continued)

State	Citation	Mentions Technology	Requires Technology	Limits Technology	Description
Oregon	2014 Or. Laws Ch. 93 § 1 “Task Force on School Safety”	No	No	No	Establishes the Task Force on School Safety
	Or. Rev. Stat. § 339.331	No	No	No	Creates the Center for School Safety within the Oregon University System serving as a clearinghouse for information and materials concerning school violence prevention and intervention services
Pennsylvania	24 Pa. Cons. Stat. § 13-1302-A	Yes	Yes	No	Establishes Office of Safe Schools within the Department of Education; authorizes the Office to make grants to schools to fund “security planning, purchase of security-related technology, which may include metal detectors, protective lighting, surveillance equipment, special emergency communications equipment, electronic locksets, deadbolts and theft control devices and training in the use of security-related technology”
Puerto Rico	P.R. Laws Ann. tit. 18, § 13	Yes	Yes	No	Requires school security plans; authorizes installation of video cameras and alarm systems in unsafe schools
	P.R. Laws Ann. tit. 18, § 17	Yes	No	No	Authorizes funds for implementation of security initiatives in schools, including the installation of security devices
	P.R. Laws Ann. tit. 18, § 141d	No	No	No	Defines powers and functions of a school security corps
	P.R. Laws Ann. tit. 18, § 2304	No	No	No	Requires church-schools to coordinate safety plans with the pertinent government agencies
Rhode Island	R.I. Gen. Laws § 16-21-23; R.I. Gen. Laws § 16-21-23.1; R.I. Gen. Laws § 16-21-24	Yes	Yes	No	Requires a comprehensive school safety plan regarding crisis intervention, emergency response and management; school safety plans shall include policies and procedures relating to security devices or procedures and internal and external communication systems
South Carolina	S.C. Code Ann. § 59-5-65	Yes	No	No	Authorizes State Board of Education to develop a model safe schools checklist, which shall include a comprehensive safety plan and emergency communication and management procedures
	S.C. Code Ann. § 59-66-30	Yes	Yes	No	Mandates that each public school in the State be equipped with one hand-held metal detector
South Dakota	None				
Tennessee	Tenn. Code Ann. § 49-6-804 & 805	No	No	No	Requires each local educational agency to adopt a comprehensive district-wide and building-level school safety plan for crisis intervention, emergency response and emergency management, which shall include policies relating to security devices
Texas	Tex. Educ. Code § 37.108	No	No	No	Requires school districts to adopt and implement a multi-hazard emergency operations plan
	Tex. Educ. Code § 37.1081 & 37.1082	No	No	No	Authorizes Texas School Safety Center (TxSSC) to develop a school safety certification program and establishes School Safety Task Force.

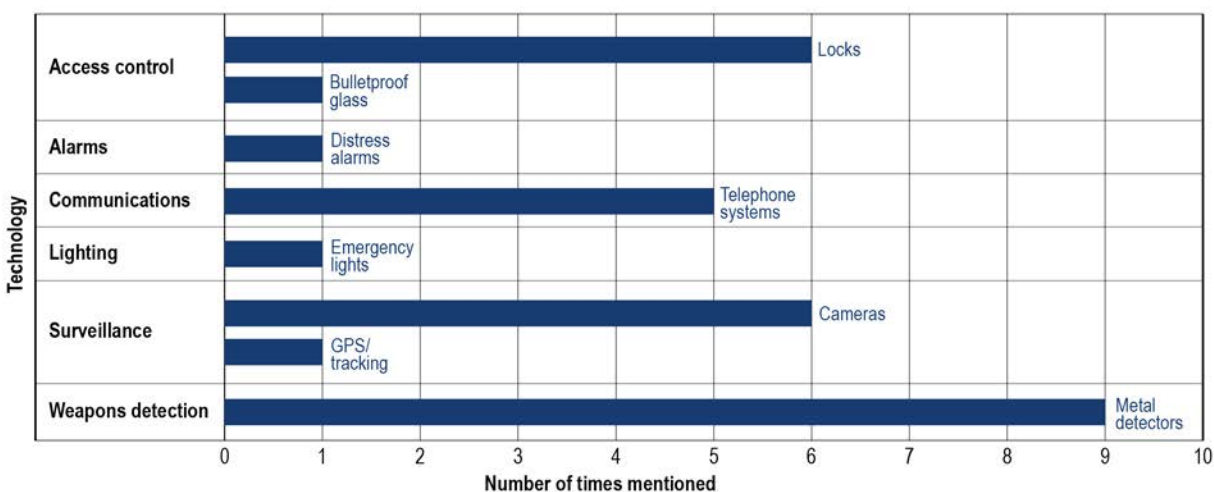
Table 12-1 U.S. Federal and State Statutes and Regulations on School Safety (Continued)

State	Citation	Mentions Technology	Requires Technology	Limits Technology	Description
U.S. Virgin Islands	None				
Utah	Utah Code Ann. § 53A-3-402	No	No	No	Requires school boards to adopt a comprehensive emergency response plan to prevent and combat violence in public schools; plan must coordinate with local law enforcement and public safety agencies
Vermont	Vt. Stat. Ann. tit. 16 § 1481	No	No	No	Requires monthly emergency preparedness drills in accordance with the school's emergency preparedness plan
Virginia	Va. Code Ann. § 22.1-279.4	No	No	No	Requires local school boards to establish threat assessment teams consistent with model policies of Virginia Center for School and Campus Safety
	Va. Code Ann. § 22.1-279.8	No	No	No	Defines school crisis, emergency management, and medical emergency response plans; requires annual school safety audits
	Va. Code Ann. § 9.1-102	No	No	No	Grants Department of Criminal Justice Services authority to establish compulsory minimum standards for school safety officers
	Va. Code Ann. § 9.1-184	No	No	No	Establishes Virginia Center for School and Campus Safety; imposes duty to provide schools with a model policy for the establishment of threat assessment teams
Washington	Wash. Rev. Code Ann. § 28A.320.125	No	No	No	Requires school districts to develop comprehensive safe school plans
West Virginia	W. Va. Code Ann. § 18-9F-1	No	No	No	Expresses legislative intent that schools must have comprehensive crisis response plan
	W. Va. Code Ann. § 18-9F-9	No	No	No	Requires state board of education to establish an "up-to-date, school specific crisis response plan at every school in the state"
Wisconsin	Wis. Stat. Ann. § 118.07	No	No	No	Requires a school safety plan
Wyoming	Wyo. Stat. Ann. § 35-9-505	No	No	No	Requires monthly fire and safety drills in all public and private schools
State Regulations (N = 17)					
Connecticut	Conn. Agencies Regs. § 14-275a-78	Yes	Yes	No	Authorizes use of optional video cameras on school busses
Indiana	Ind. Admin. Code tit. 511, r. 6.1-2-2.5	No	No	No	Defines minimum standards for written emergency preparedness plans
Louisiana	La. Admin Code tit. 28, pt. CXV, § 339	No	No	No	Defines duty of principal or school leader with regard to crisis management and response plan
Maine	05-071 Me. Code R. 125 § 10	Yes	No	No	Mandates each school administrative unit to develop a Crisis Response Plan; school personnel shall have access to a "telephone or other means of electronic communication"
Maryland	Md. Code Regs. 13A.02.02.01 et seq.	No	No	No	Sets forth requirements for emergency plans in local school system
Nebraska	Neb. Admin. R. & Regs. tit. 92, Ch. 10, § 011	No	No	No	Requires each school system to have a safety and security plan for schools in the system

Table 12-1 U.S. Federal and State Statutes and Regulations on School Safety (Continued)

State	Citation	Mentions Technology	Requires Technology	Limits Technology	Description
New Jersey	N.J. Admin. Code tit. 6A § 16-5.1	No	No	No	Requires each school district to develop and implement comprehensive plans, procedures, and mechanisms that provide for safety and security in the public schools
	N.J. Admin. Code tit. 6A § 16-5.3	No	No	No	Requires incident reporting of violence in school
New Mexico	N.M. Admin. Code tit. 6 §12.6	No	No	No	Requires adoption of local school district wellness policies that must include, as a component of the school safety plan, an Emergency Operations Plan
New York	N.Y. Comp. Codes R & Regs. tit. 8, § 100.2	No	No	No	Provides for promulgation of standards and procedures to assure the security and safety of students and school personnel [§100.2(l)(2)(ii)(c)]
	N.Y. Comp. Codes R. & Regs. tit. 8, § 155.17	No	No	No	Requires each board of education of a school district to prepare a district-wide and building-level school emergency management plan
Ohio	Ohio Admin. Code § 3301-5-01	No	No	No	Defines the requirements of the comprehensive emergency management plan
Oregon	Or. Admin. R. 581-022-1420	No	No	No	Requires school districts to maintain a comprehensive emergency plan and safety program
Pennsylvania	22 Pa. Code § 10.24	No	No	No	Requires school districts to develop and implement a comprehensive disaster response and emergency preparedness plan
Rhode Island	R.I. Code R. 31-1-37:37.0	Yes	No	No	Defines the requirements of school safety plans; requires policies and protocols for use of emergency communication systems
Texas	40 Texas Admin. Code § 744.3551 et seq.	Yes	Yes	No	Defines the requirements of Emergency Preparedness Plans; requires telephone communication system, child tracking system, and personnel tracking system
Utah	Utah Admin. Code R277-400	Yes	Yes	No	Establishes criteria for Emergency Preparedness and Emergency Response Plan; requires access planning and control
Virginia	8 Va. Regs. Reg. 20-131-260	No	No	No	Establishes school safety standards; requires written procedure for responding to violent activities
West Virginia	W. Va. Code St. R. tit. 164, 6-3	No	No	No	Directs School Building Authority to incorporate safe school design into new schools

Note: Only states and territories with relevant school safety/technology regulations are listed in the table. No tribal jurisdictions were found to have relevant school safety/technology statutes or regulations and are excluded from the table as well.



Note: Technologies not listed in the figure were not mentioned specifically in any federal or state statutes or regulations.

15-03015-004

Figure 12-1 Types of Technologies Covered in Federal and State Statutes and Regulations

12.2.3.2 State-Level Statutes

Forty-nine jurisdictions, including the District of Columbia, Guam, and Puerto Rico, have passed laws that require the adoption of a school safety or security plan in addition to the Federal requirement. More specifically, the law in 23 of these jurisdictions (22 states and Puerto Rico) prescribes the application of some type of technology as part of a comprehensive school safety, crisis response, or emergency preparedness plan. Four states (Hawaii, Idaho, North Dakota, and South Dakota) do not require schools to adopt or implement a school safety plan. To the extent that tribal jurisdictions, the U.S. Virgin Islands, and the Northern Mariana Islands were included in the legal database search, no relevant results were returned. See Figure 12-2.

Among the 85 state statutes, 32 statutes in 23 state and territorial jurisdictions make reference to the use or application of technology to improve school safety and security. Among the state statutes that reference technology, 17 require that certain technologies be included as part of a school district's safety plan. Only two jurisdictions, Delaware and Louisiana, make specific statutory reference to Fourth Amendment protections that would place any limit or restriction on the use of those technologies for school safety.

In jurisdictions that have legislated the use of specific technologies, the requirement for technology is generally only one element of a more comprehensive school safety or crisis response plan. When technology is prescribed, the focus tends to be on weapons detection, access control, communications, and surveillance technologies. South Carolina and Delaware, for example, specifically allow the use of metal detectors¹ in schools, but also require comprehensive, site-specific safety plans.² Montana requires the adoption of an emergency operations plan and that it include a communication system.³ Georgia, Mississippi, and Pennsylvania permit discretion by the local school boards to decide among a range of options for security-related technology devices, including video surveillance cameras, communications equipment, and electronic locks. Alaska requires a communication and lockdown plan, which may involve the use of technology, to be a part of all school-specific crisis response plans, but no

¹ 14 Del. C. § 4119; S.C. Code Ann. § 59-66-30.

² 29 Del. C. § 8237; S.C. Code Ann. § 59-5-65.

³ Mont. Code Ann. § 20-1-401.

details regarding such plans are provided. In April 2015, the Arkansas legislature enacted a bill that requires local schools to install a panic button alert system on or before 1 September 2015, provided funding is available.⁴

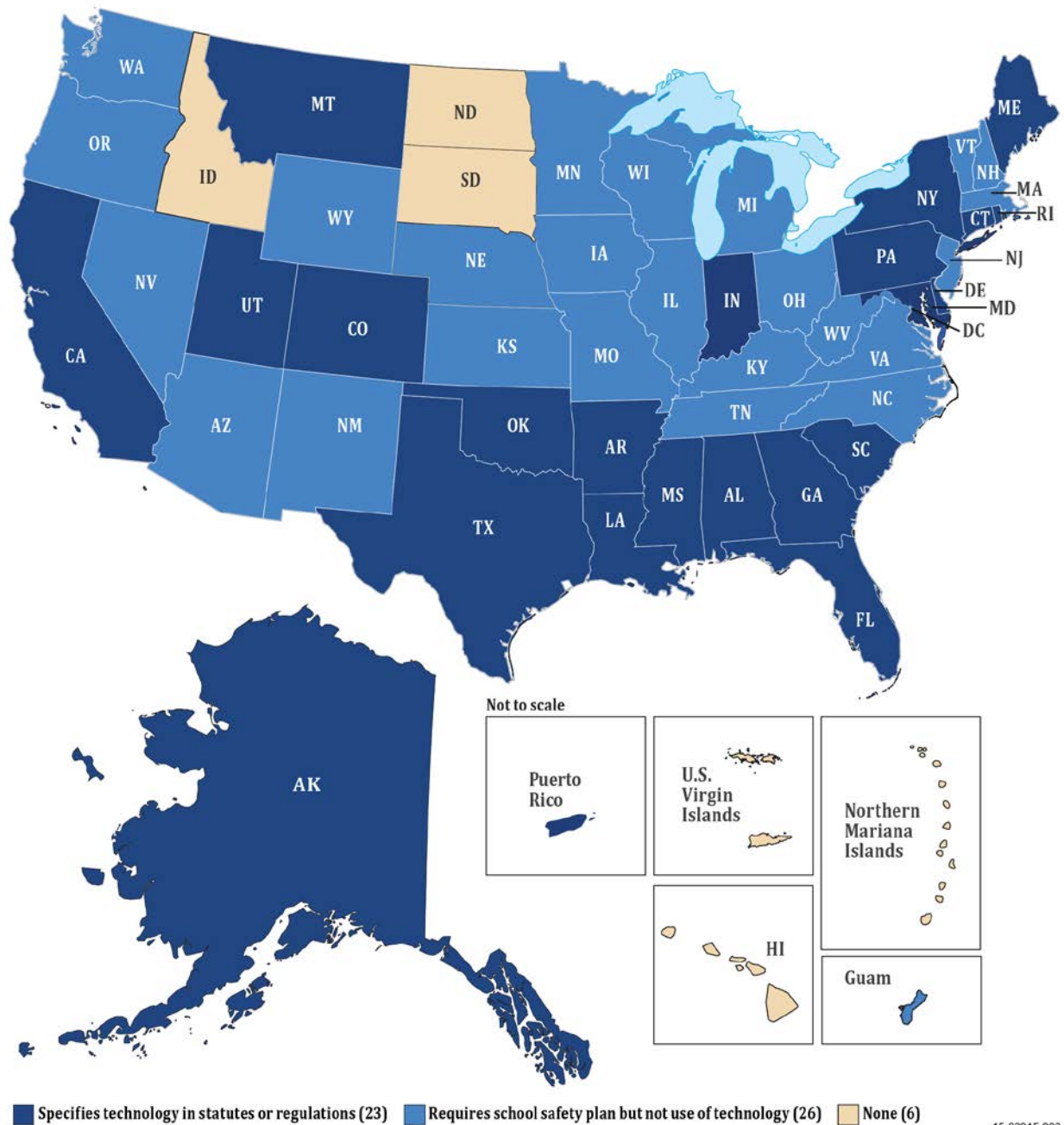


Figure 12-2 Map of State Statutes and Regulations Requiring School Safety Plans or Specific Technology

⁴ Ark. Code Ann. § 16-15-1302.

Connecticut has established a School Safety Infrastructure Council mandated to develop school infrastructure standards regarding a wide range of technologies, such as reinforced entryways and doors, ballistic glass, computer-controlled electronic locks, surveillance cameras, and “other security infrastructure improvements and devices as they become industry standards.”⁵ In addition, each local board of education is required to implement an all-hazards approach safety plan that complies with the protocols of the National Incident Management System (NIMS).⁶ The NIMS is a standardized emergency preparedness protocol developed by the Department of Homeland Security that establishes a systematic, proactive approach to reducing the loss of life and property and/or harm to the environment as a result of an emergency situation or incident. While NIMS is not directed solely toward technology, when entities are creating their NIMS plan, they are likely to consider the use of technology.

Delaware, Colorado, and New Hampshire have also adopted the NIMS approach to incident management. Delaware, in addition to authorizing the use of video cameras and metal detectors, requires that public schools establish comprehensive, site-specific, NIMS-compliant emergency preparedness plans.⁷ In 2008, the Colorado legislature created the Colorado School Safety Resource Center to provide technical assistance to schools in developing or implementing safety and preparedness plans. The Resource Center has established an extensive framework for school emergency incident response, which includes the adoption and implementation of NIMS-compliant safe school plans.⁸ New Hampshire mandates that every public and nonpublic school develop a site-specific emergency response plan that conforms to the Incident Command System and the NIMS.⁹

Communities that employ NIMS practices “are part of a comprehensive national approach that improves the effectiveness of emergency management and response personnel across the full spectrum of potential threats and hazards (including natural hazards, terrorist activities, and other human-caused disasters) regardless of size or complexity” (Reference 113). State statutes that have incorporated the NIMS approach for managing incidents need not specify the use of any particular technology. The U.S. Department of Education provides further guidance on how technology can be used to comply with NIMS requirements for school safety (Reference 358).

Some jurisdictions do not specify the use of certain technology or target-specific technologies to be included in the general school safety plan, but rather grant broad authority to the state board of education or local school district to adopt immediate and long-term strategies that address school safety and leave the scope of the plan to be developed by the school principal or other local policymakers. In Arizona, the governing boards of local school districts are empowered to develop emergency response plans in accordance with minimum standards jointly established by the state department of education and the division of emergency management within the department of emergency and military affairs.¹⁰ In North Carolina, the principal of each school leads a school improvement team to develop a site-specific safety plan and the team may seek technical assistance from the local board of education.¹¹

The West Virginia state board of education also provides a model plan and uniform template for local schools to follow.¹² Although the model plan must be developed in conjunction with the Division of

⁵ Conn. Gen. Stat. Ann. § 10-292r(b).

⁶ Conn. Gen. Stat. Ann. § 10-222n. See www.fema.gov.

⁷ 29 Del. C. § 8237

⁸ Colo. Rev. Stat. Ann. § 22-32-109.1

⁹ N.H. Rev. Stat. Ann. § 189.64

¹⁰ Ariz. Rev. Stat. § 15-341.A.32

¹¹ N.C. Gen. Stat. Ann. § 115C-105.33

¹² W. Va. Code Ann. § 18-9F-9

Homeland Security and Emergency Management and shall include comprehensive protocols for responding to the physical harms suffered by students, safe entrance and exit procedures, and policies for enforcing school discipline during a crisis, the statute does not recommend or prescribe specific technologies for the school board to include in its model plan. The Illinois School Safety Drill Act sets forth minimum standards for schools to follow in reviewing school emergency and crisis response plans,¹³ but with no further legislative guidance, encourages school administrators to develop plans that exceed the requirements and standards set forth in the statute.¹⁴

Iowa and Massachusetts allocated funds for upgrades in school infrastructure. Iowa sets aside Federal funds for the school budget review committee to develop a school infrastructure safety fund grant program, in conjunction with the state fire marshal.¹⁵ Massachusetts incorporates “upgrades and technological devices necessary for enhanced [school] safety and security” into the allowable costs for approved school construction or renovation projects.¹⁶

Some jurisdictions, among them the District of Columbia, Kentucky, Maryland, Minnesota, Nebraska, Oregon, Oklahoma, Texas, Virginia, and Guam, have established by statute a school safety council, coordinator, or task force to provide technical assistance and to coordinate the jurisdiction’s approach to ensuring a safe school environment. Like the National Center for School and Youth Safety,¹⁷ these task forces or centers for school safety serve as a central repository of information for: best practices and are responsible for coordinating resources; providing training, oversight, and evaluation of school safety programs; analyzing data and disseminating best practice information; and promoting inter-agency and private sector partnership to ensure a safe and secure school environment.

Texas requires each school district to adopt a “multihazard emergency operations plan” and grants authority for periodic review and audit of the plans to the Texas School Safety Center (TxSSC).¹⁸ The TxSSC bases its model emergency operations plan on the NIMS and recommends that independent school districts in Texas adopt NIMS to manage all situations involving natural or human-caused disasters or terrorist events.¹⁹

In Virginia, the Center for School and Campus Safety issued a school safety inspection guide in 2014 for all public schools in Virginia.²⁰ This guide provides a walk-through inspection checklist to be used as part of the overall school safety audit. The checklist identifies areas of vulnerability and includes recommendations for best practices. For example, if surveillance cameras are to be installed, the Center recommends that school administrators designate an individual to be responsible for viewing surveillance recordings, changing the storage media, and storing the recordings. There are additional suggestions with regard to technologies that might be used to enhance school safety, including security alarm systems, signage and entrances, doors, windows, key control, emergency lights and interior

¹³ 105 Ill. Comp. Stat. Ann. § 128/1 et seq.

¹⁴ 105 Ill. Comp. Stat. Ann. § 128/10.

¹⁵ Iowa Code § 423E.6

¹⁶ Mass. Gen. Laws Ann. ch. 70B § 14.

¹⁷ 20 USC. § 7138. Congress specifically authorized funds for the Secretary of Education and the Attorney General, to jointly establish a National Center for School and Youth Safety, with a mandate to “compile information about the best practices in school violence prevention, intervention, and crisis management, and shall serve as a clearinghouse for model school safety program information.”

¹⁸ Texas Education Code § 37.108.

¹⁹ See the TxSSC website and the Sample-District-EOP. Retrieved from <https://txssc.txstate.edu/tools/emergency-management-toolkit/role-of-districts/multi-hazard-eop/>

²⁰ 2014 School Safety Inspection Checklist for Virginia Public Schools. Retrieved from <http://www.lcps.org/cms/lib4/VA01000195/Centricity/Domain/126/14SchoolSafetyInspectionChecklist.pdf>

lighting, identification badges, two-way communication systems, the use of convex mirrors in hallways, and tempered observation panels in classrooms.

Only two jurisdictions specifically limit the use of security-related technology with regard to school safety, and these legislative restrictions are narrowly tailored to address Fourth Amendment privacy concerns. Delaware authorizes the use of video cameras for surveillance on public school property, but requires the consent of the principal and teacher if video cameras are to be used to monitor student behavior in the classroom. Moreover, Delaware specifically prohibits the use of cameras “at any time or in any location which could violate a student’s reasonable expectation of privacy, including but not limited to, locker rooms, areas where students may disrobe, and lavatories.”²¹ Similarly, city and parish school boards in Louisiana are permitted to install metal detectors in elementary and secondary schools; however, safety plans that include the use of metal detection devices for random weapon searches are subject to the approval of the state attorney general.²² Additionally, the local school boards must provide training on the proper use of metal detectors and other techniques for weapon searches.²³

12.2.3.3 State-Level Regulations

Among the 17 state regulations identified, 5 specify a particular category of technology that must be employed as part of school safety standards and security procedures. Maine requires school personnel to have “ready access to a telephone or other means of communication....”²⁴ Rhode Island’s school safety plans must include a formalized collaborative arrangement with state and local professional public safety agencies, and law enforcement and emergency personnel, and have emergency communication systems and protocols in place in the event of a violent incident.

In Utah, each school board is required to develop the general criteria for emergency preparedness and to implement a response plan to prevent and combat violence in the public schools. The LEA in Utah must develop and maintain adequate prevention, intervention and response measures.²⁵ Such security measures are required to address “access planning,” but that term is not defined in the regulation nor does the regulation specify any particular technical applications to include in such a plan.

In Texas, the TxSSC has quasi-regulatory authority with respect to the oversight of safety plans in the independent school districts. Notably, however, the Texas Department of Family and Protective Services promulgated emergency preparedness regulations providing minimum safety standards for school-age children in before- and after-school programs.²⁶ The regulations address, although not in detail, the need for a communication system, a child tracking system,²⁷ and emergency lighting systems.²⁸

In New Jersey, each school district is required to have a comprehensive school safety and security plan developed in cooperation with local law enforcement, public health officials, and emergency management agencies.²⁹ Although the regulation is silent as to the technology required by the school

²¹ 14 Del. C. § 1421.

²² La. Rev. Stat. Ann. § 17:81.

²³ Id.

²⁴ 05-071 Me. Code R. 125 § 10.

²⁵ Utah Administrative Code R277-400.

²⁶ 40 Texas Admin. Code § 744.3551 et seq.

²⁷ Id. at § 744.3553.

²⁸ Id. at § 744.3565.

²⁹ N.J.Admin.Code tit. 6A § 16-5.1.

safety plan, it is clear that the plan must be consistent with the format and content established by the New Jersey Domestic Security Preparedness Task Force.³⁰

New Jersey has taken a different approach compared to most other states. Since the late 1980s it has recognized the need to ensure the safety and security of its schools with much of the work accomplished over the years by the cooperative efforts of state agencies, task forces and working groups appointed by executive action, legislation, and regulation.³¹ In 2013, a School Security Task Force was convened to identify “physical and cyber vulnerabilities and potential breaches of security in New Jersey’s public schools and to make recommendations to improve school safety and security.”³² The Task Force specifically looked at technologies that included: screening systems at school entrances; advanced identification card systems for students, employees, and visitors; biometric, retina, and other advanced recognition systems for authorized entrance to schools; panic alarms; the hardening of school perimeters; and emergency communications plans.³³

Of primary importance among the numerous recommendations made by the Task Force was that New Jersey legislatively establish “a permanent and fully funded New Jersey School Safety Specialist Academy under the aegis of the Department of Education (DoED), as a central repository for best practices, training standards, and compliance oversight in all matters regarding school safety and security.” The Task Force recommended that the state, either through legislation or regulation, require communication systems in schools, including two-way radios and emergency notification platforms, advanced student and visitor identification cards with a computerized access control system, and the hardening of school perimeters and building entryways using electronic door locks, video surveillance cameras, lighting systems, and ballistic or shatter resistant film on glass doors and windows. The Task Force did not think it prudent to recommend panic alarms or biometric, retina, or other advanced recognition systems. Recognizing the strengths and limitations of the various screening systems alternatives, the Task Force recommended that the decision to install and use screening devices be left to the discretion of each school district.

12.2.3.4 Aggregate Results at the State and Federal Level

Table 12-2 presents the percent of states and territories with school safety statutes or regulations that mention, require, or limit the use of technology for school safety. At the Federal level, the five Federal statutes taken as a whole mention technology and both place requirements and limitations on its use. The Federal statutes also specify implementation deadlines and funding mechanisms for those requirements. The only limitation stipulated by statute on the use of technology for the purpose of advancing or promoting school safety is that of Fourth Amendment privacy concerns.

³⁰ See N.J.S.A. § App. A:9-64 et seq. The Task Force was created by the New Jersey Domestic Security Preparedness Act (P.L. 2001, c. 246) after the September 11, 2001 terrorist attack. Chaired by the state’s Attorney General, the Task Force is responsible for the coordination and supervision of all activities related to domestic preparedness policy, including Pre-K through grade 12 public schools.

³¹ For a summary of significant legislation and other actions related to school security in New Jersey taken from 1988 to the present, see, New Jersey School Security Task Force Report, July 2015, downloaded from www.nj.gov/education/schools/security/TaskForceReport.pdf.

³² Id.

³³ Id.

Table 12-2 Federal and State Statutes and Regulations Regarding School Safety in the United States

	Federal Statutes (N = 5)	States with Statutes (N = 49*) N (%)	States with Regulations (N = 17**) N (%)
Statutes and regulations that mention technology	Yes	20 (41)	5 (29)
• If yes, specifies funding mechanism or amount	Yes	10 (20)	0 (0)
• If yes, specifies implementation deadline	Yes	15 (31)	2 (12)
• If yes, specifies technology for school buses	Yes	1 (2)	1 (6)
Requires technology of some kind in schools	Yes	15 (31)	3 (18)
• If yes, specifies funding mechanism or amount	Yes	9 (18)	0 (0)
• If yes, specifies implementation deadline	Yes	10 (20)	1 (6)
Limits technology for school safety	Yes	2 (4)	0 (0)
• If yes, specifies 4th Amendment concerns	Yes	1 (2)	0 (0)

*Includes the following states and territories with relevant statutes: AL, AK, AZ, AR, CA, CO, CT, DE, DC, FL, GA, Guam, IL, IN, IA, KS, KY, LA, ME, MD, MA, MI, MN, MS, MO, MT, ME, MV, NH, NJ, NM, NY, NC, OH, OK, OR, PA, Puerto Rico, RI, SC, TN, TX, UT, VA, VT, WA, WV, WI, and WY.

**Includes the following states with relevant regulations: CT, IN, LA, ME, MD, NE, NJ, NM, NY, OH, OR, PA, RI, TX, UT, VA, and WV.

Among the 49 jurisdictions identified that have enacted legislation that addresses school safety, 20 jurisdictions (41%) mention technology, 10 jurisdictions (20%) specify the funding mechanism or amount for school safety provisions, and 15 jurisdictions (31%) specify the implementation deadline. Fifteen (31%) of the 49 jurisdictions with relevant statutes require technology of some kind in schools, eight (18%) specify funding for that required technology and 10 (20%) specify the implementation deadline. Only two (4%) of the states have statutes that place limits on technology, and one of the two (2%) cites Fourth Amendment privacy concerns as the reason for those limitations.

Among the 17 states with regulations covering school safety, five mention technology, and two specify the implementation deadline for components of the school safety regulation. Three of the 17 states with relevant regulations require technology of some kind for school safety, and one state specifies an implementation deadline for those requirements.

12.2.3.5 School Bus Safety

A few states have contemplated the need for guidance with respect to a violent or traumatic event occurring on a school bus and have included provisions in their school safety laws to address technology on buses. Arizona requires its public school districts to include policies in their school safety plans that prohibit bullying through the use of electronic technology or electronic communication on school property and, specifically, on school buses. School officials must develop a formal process for the investigation of suspected incidents of cyber-bullying and design procedures to monitor and protect the health and safety of their students. Colorado school districts must develop general policies and

procedures for dealing with disruptive students on school buses.³⁴ Illinois requires school bus evacuation drills, but does not specify what, if any, technology is required to facilitate such safety drills. The Connecticut Department of Motor Vehicles permits optional video cameras to be installed on school buses provided the camera be mounted in such a way that it does not encroach on the headroom of the entrance or aisle and does not limit ingress or egress by the bus driver.³⁵

12.2.3.6 Local Laws and Policies

As previously stated, the research team also examined the publicly available information provided on the websites of 25 local school districts throughout the country.³⁶ The team was able to obtain information from 21 of those localities. These school districts constitute a convenience sample, which was derived from media analysis.

Of the 21 school district websites reviewed, the team noted a relatively low level of detail among most, with a few notable exceptions. Naperville Community Unit School District 203 in Illinois issued a clear policy with regard to the use of video cameras for the monitoring of individuals in its school buildings and on district property.³⁷ The policy clarifies that the “purpose of such cameras is for student safety and security” and requires school facilities with video surveillance cameras to “display a warning sign at the main entrance indicating that video surveillance can occur in that facility to provide for security of school facilities and District property, to ensure student safety, and to encourage proper student behavior.”³⁸ The policy places limits on where video cameras may be located and how long recordings may be kept, and specifies that the information recorded is for official use only.³⁹ Naperville also permits electronic visual and audio recordings on school buses to monitor conduct. Notice of the recording must be prominently displayed and may be used as evidence in a student disciplinary proceeding.⁴⁰

Buncombe County in North Carolina has developed a detailed system-wide safe school plan that addresses mitigation and prevention, preparedness, response, recovery, and evacuation and reunification.⁴¹ The plan provides a comprehensive list of actions taken by the school system to ensure the welfare of the school community. With respect to school safety technology, the safety plan states that a video security system has been designed and that an electronic blueprint of all campuses in the Buncombe County school system has been developed. The safety plan specifies that the county uses the Incident Command System and includes a detailed explanation of what that system is and what it is intended to do in the event of an emergency. It provides that emergency response kits shall be maintained in each county school and specifies a list of items that shall be included in the kit. Lastly, the plan sets forth the methods of communication that shall be standard in the county in an emergency event, which includes the School Messenger Rapid Notification Service and the Seven Kenwood Model TK-272G two-way handheld devices that allow for communication between the school and 12 emergency response channels representing the county emergency management, fire department, and

³⁴ Colo. Rev. Stat. Ann. § 22-32-109.1(2)(a)(B).

³⁵ Conn. Agencies Regs. § 14-275a-78

³⁶ The team reviewed local school board policies in the following states: California, Colorado, Florida, Illinois, Maryland, New Jersey, New York, North Carolina, North Dakota, Oregon, Texas, and Virginia.

³⁷ Naperville Community School District 203 Policy Manual. Downloaded from http://policy.microscribepub.com/cgi-bin/om_isapi.dll?clientID=2826891684&depth=2&infobase=naperville.nfo&softpage=PL_frame.

³⁸ Id.

³⁹ Id.

⁴⁰ See http://policy.microscribepub.com/cgi-bin/om_isapi.dll?clientID=2826891684&depth=2&infobase=naperville.nfo&softpage=PL_frame

⁴¹ Buncombe County Schools, System-wide Safe School Plan (Part B), downloaded from <http://www.buncombe.k12.nc.us/cms/lib5/NC01000308/Centricity/Domain/42/PART%20B-FOR%20ON%20LINE.pdf>.

sheriff's department; and cellular phones networked among school principals and central incident command office staff.

In some instances within this small sample, the team found that written policies at the local school district level that are available to the public tend to be restatements of general policy rather than detailed operations manuals outlining the precise procedures to be followed in case of emergency. For example, in New Jersey, the Plainfield Community Consolidated School District 202 safety manual states that the school district shall have a comprehensive safety and crisis plan that incorporates both avoidance and management guidelines for instances of injury prevention, bomb threats, weapons, and explosives on campus and that there must be regular school safety drills conducted with the participation of the appropriate law enforcement agency.⁴² School regulations in Montgomery County in Maryland are similar in scope, noting that schools must comply with Federal and state requirements for emergency planning and preparedness, collaborate amongst divisions to provide technical assistance to schools, and conduct six emergency preparedness drills each year. Likewise, the Los Angeles Unified School District policy reinforced the duty of the superintendent of schools to comply with the requirements of California law with regard to safety in schools.

More detailed information and technical specification is likely to be available to school administrators than is made available on public websites. Publicly available policy manuals and guidance documents, however, are only slightly more instructive than the minimum safety requirements set forth in most states' statutes.

12.2.3.7 Newspaper Coverage

The news media coverage provides an additional lens through which the team examined both the use of technology for school safety as well as public attitudes about safety measures in schools. The sample consisted of 168 articles covering school safety from January 2010 through June 2015. Of those, 102 articles (61%) mentioned the use of technology for school safety. Figure 12-3 presents the sample of newspaper coverage included in this study.

The frequency with which different technologies were discussed in news coverage and whether that coverage was purely factual (no opinion expressed) or if positive, negative, or both positive and negative opinions were expressed about that technology, is presented in Figure 12-4. Access control technologies were the most frequently discussed in news coverage about school safety (74% of articles) followed by surveillance technologies (63% of articles), communications technologies (26% of articles) and alarms technologies (24% of articles) and weapons detection technologies (21% of articles). Cyber systems and lighting technologies were discussed the least frequently (in 10% and 4% of articles respectively).

⁴² Board Policy Manual Plainfield Community Consolidated School District 202. Retrieved from <http://www.psd202.org/files/EdCeJ/902610ba42a1b0bb3745a49013852ec4/manual>.

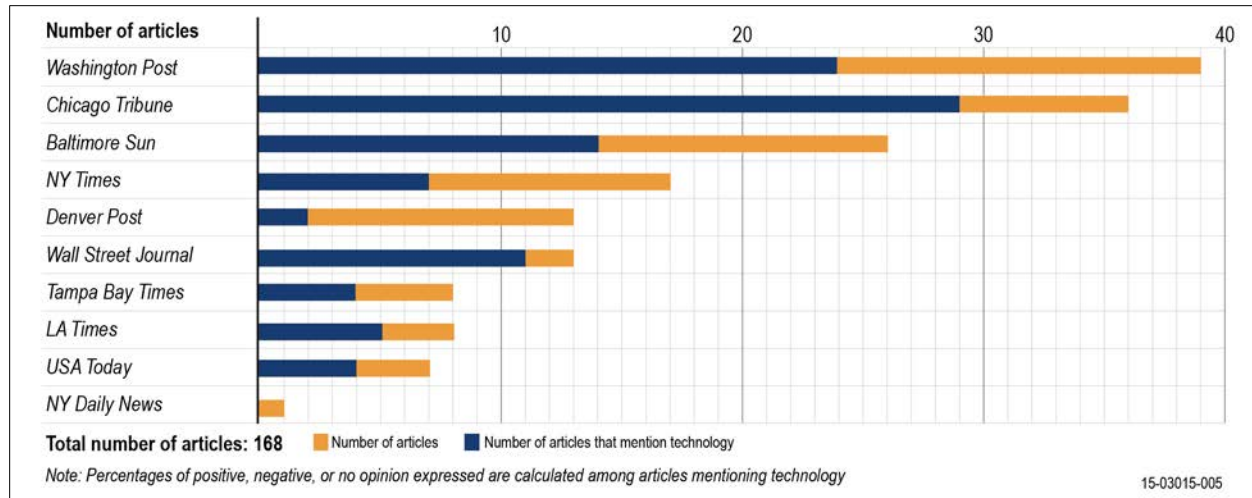


Figure 12-3 Number of Articles Covering School Safety and Technology from 2010 to 2015 in Selected U.S. Newspapers

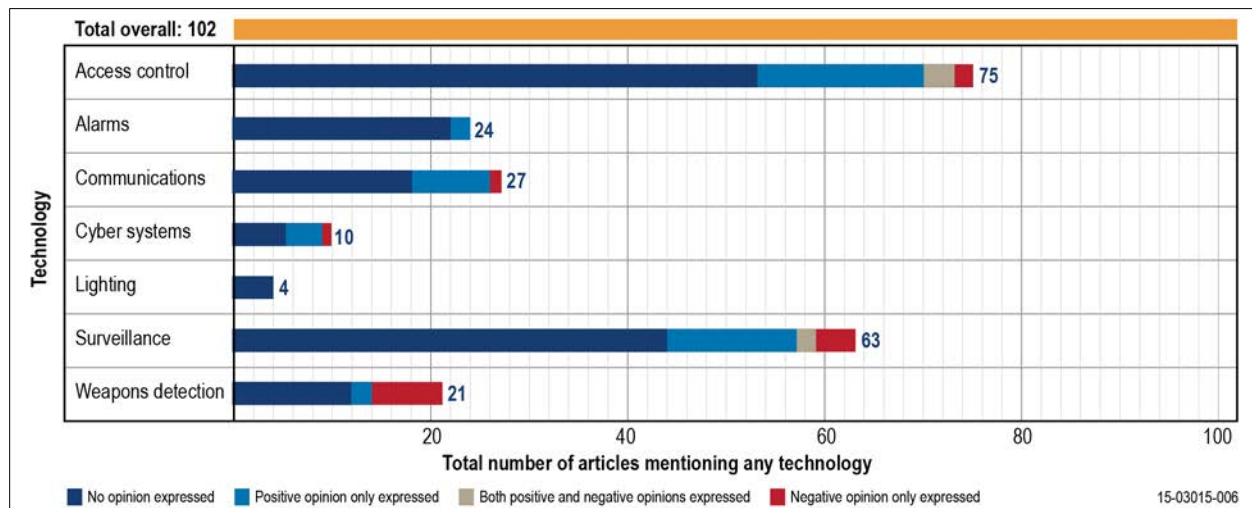


Figure 12-4 Technology in Context of School Safety in Major U.S. Newspaper Articles 2010 to 2015 Among Articles that Mentioned any Technology (N = 102)

The number and percent of articles that contained specific supportive and opposing messages about technology in schools is presented in Figure 12-5. The majority of articles were factual and did not include opinions on the use of specific technologies. However, when opinions were expressed they were generally positive. Negative opinions were expressed in very few instances and expressions of both positive and negative opinions in the same article were rare. Fifty-four percent of the articles included messages about technology being needed in response to a specific mass shooting incident. For instance, the shooting at Sandy Hook Elementary School was frequently mentioned, as were the Columbine and Aurora shootings. Seventeen percent of articles stated that technology was necessary because of general trends of increasing school violence.

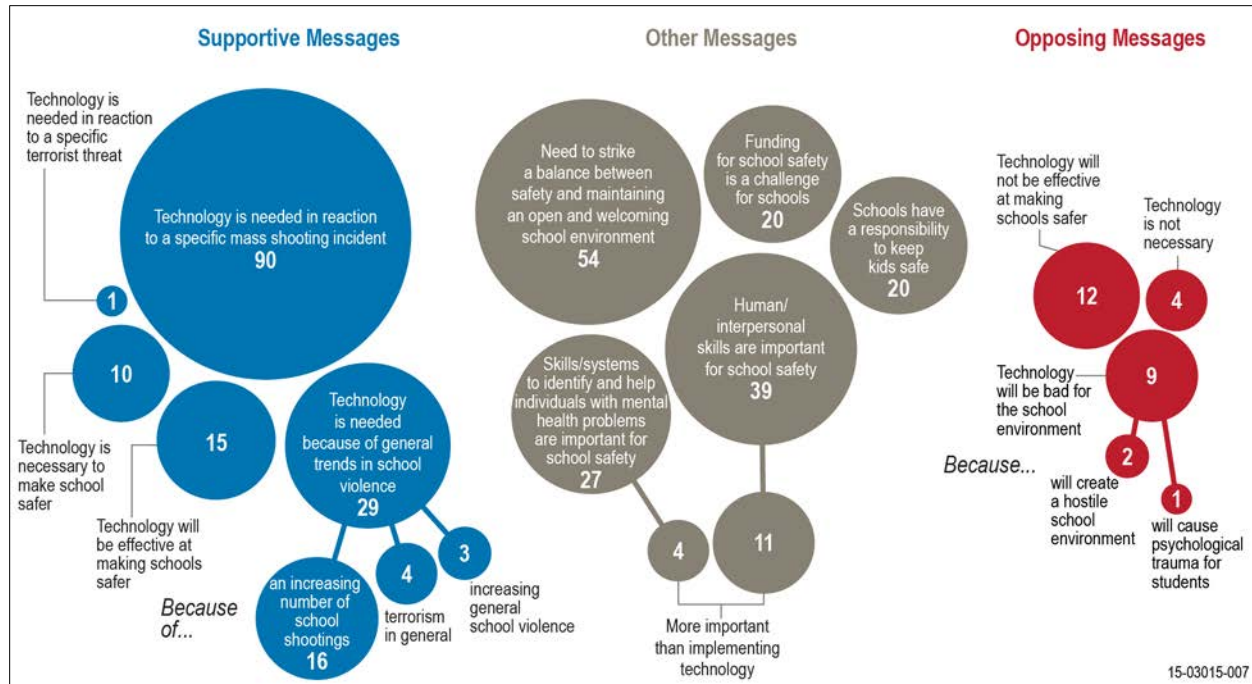


Figure 12-5 Contextual Messages About Technology Use in Major Newspaper Coverage of School Safety from 2010 to 2015, Overall (N = 168)

Few articles included messages about the effectiveness of technology for school safety. Nine percent included messages about technology being effective at making schools safer, and 7% included messages about technology not being effective at making schools safer. Five percent of articles included statements about technology being detrimental to the overall school culture or learning environment.

One third (32%) of articles on school safety discussed the need to strike a balance between safety and maintaining an open and welcoming school environment. Articles also contrasted the importance of technology with the importance of human or interpersonal skills in keeping school safe (23% of articles) and the need for skills and systems to identify and help individuals with mental health problems (16%).

12.3 DISCUSSION

In this study, the research team used legal research methodology to examine the extent to which Federal, state, territorial, and tribal laws and regulations mandate or place limits on the use of technology in schools for the prevention of violence. The team also examined news media coverage of technology and school safety between January 2010 and June 2015 in a selection of U.S. newspapers. Overall, the legal research demonstrates that legislators and regulators at the Federal and state levels are concerned with school safety and have taken steps to codify those concerns in legislation, regulation, and other policies. However, few of these laws mention specific technologies and even fewer mandate their use. Media research suggests that some school districts have gone beyond what is legally required and have implemented technologies to enhance school safety.

Laws at the Federal and state levels, in general, create an obligation for schools to have safety plans, but with few exceptions they do not specify types of technology allowed or required. State-level statutes and regulations offer little guidance or specificity as to how to ensure the safety of the school or the role that technology should play in school safety. One possible reason for this is that technology develops

quickly and is always changing, whereas law generally lags considerably behind the available technology and the process by which new laws or regulations are created is slow by comparison. For this reason, lawmakers may well be reluctant to specifically prescribe in their statutes the exact type of technologies that schools should employ, leaving decisions at that level of detail to the schools themselves.

Achieving the optimal balance between providing highly specific mandates in legislative enactments versus restricting legislation to broad policy statements is difficult. Lawmakers will often be deferential to those with greater knowledge of technological details, such as when lawmakers create administrative agencies to deal with the detailed implementation of broadly stated policies. The creation of the National Highway Traffic Safety Administration and the Consumer Product Safety Commission are examples, at the Federal level, of Congress calling for safety enhancement and creating agencies to deal with the technological details of how to achieve that goal.

However, in the area of school safety, no Federal regulatory agency has been created or charged with the responsibility of assessing which technologies are effective in maintaining a safe school environment. Most states also do not have an agency for assessing technologies. Some states have created centers, as discussed herein, but it is unclear how these centers share or coordinate information with each other or how they disseminate the information to a wide audience. As a result, school administrators at the local level may lack guidance in their choices of safety technology, and the broad policy statements contained in Federal and state legislation may prove inadequate in maximizing efficiency and effectiveness of the acquisition and use of school safety technologies.

With few exceptions, the statutes and regulations do not delineate specifically what school districts *must* do, but they do provide a broad framework for what they are *allowed* to do. Results from the team's media analysis suggest that, within this broad framework, schools are taking actions to protect the safety of their students and staff, often using technology such as video surveillance technology, new locks, and other access control technology. Thus, although the law may seem vague, schools are proactively implementing planning and technology-based safety measures.

The precise degree to which the current state of statutory and regulatory law on school safety (and the lack of specificity regarding the use of technology contained therein) presents a problem, and the assessment of policy options to solve the problem, is beyond the scope of this report. An adequate answer to those questions would require a detailed analysis of the effectiveness of such laws and regulations, and such an analysis would present difficult methodological problems and data collection issues.

The planning process for ensuring school safety is inherently a cooperative activity requiring partner organizations to work together. The legislative and regulatory processes are simply not nimble enough to keep up with advancements in technology or the changes in local funding availability. The research team's findings suggest that most state legislators recognize that less prescriptive policies allow local school boards and school administrators the flexibility they need to strategically implement technology and develop the site-specific protocols and procedures for ensuring the safety of their school environments. However, school administrators should be aided by objective information collected and analyzed at the Federal and/or state levels regarding the availability, cost, and effectiveness of technologies designed to protect the safety of the occupants of schools.

12.4 STRENGTHS AND LIMITATIONS

To the research team's knowledge, this is the most comprehensive undertaking of an examination of Federal and state laws and regulations regarding technology designed to reduce criminal violence in K-12 schools. Using comprehensive electronic legal databases, the team examined statutes and regulations currently in existence in all 50 states, as well as tribal jurisdictions and U.S. territories. The team further complemented this analysis with a review of media coverage of the use of technology for school safety in the highest circulation U.S. newspapers. There are, however, some possible limitations to this study.

As described in Section 12.2, the identification of statutes and regulations was largely a function of carefully selected search terms developed through an iterative process and used in the searches of electronic legal databases. Even with the deployment of broadly defined initial searches, however, it remains possible that some relevant statutes or regulations may not have been captured. Regardless, this report should be considered a snapshot of what existed at the time of the searches, with the understanding that statutes and regulations change with the passage of time, and it is difficult to ensure that 100% of all laws were included.

Because electronic legal databases do not provide access to local policy guidance documents and individual school or school district rules regarding technology and school safety, a similarly comprehensive examination was not conducted. A small sample of policies and rules were examined. It is possible that local policies outside the sample do provide detailed guidance about the use of technology in schools. However, the news media coverage analyzed mitigates some of this concern.

12.5 CONCLUSION

Law, in all of its forms, can be a useful tool in creating duties and providing guidance regarding the use of technology to best ensure safety in the country's K-12 schools. Given the Federalist system of law in the United States, by which much authority is left with the states to protect the health and safety of its citizens, one would expect to find, as this study did, wide variations in the approaches states have taken regarding technology in schools. Overall, however, states have provided policies that, in broad terms, set the clear expectation that technology can and often should be deployed, with limited restrictions involving the safeguarding of privacy rights, to enhance the safety of students, faculty, and staff in the nation's schools.

Chapter 13. LITERATURE REVIEW

Sheldon F. Greenberg, PhD

13.1 INTRODUCTION

Throughout the United States and the world, there is a rapidly increasing use of technology to ensure the safety and security of Pre-Kindergarten (Pre-K), elementary, middle, and high schools. Technology plays an integral role in the prevention and mitigation of inappropriate behavior and violent crime.

By providing a baseline perspective on school safety technology, this literature review fosters increased understanding of such technology and advances future research on the topic. To guide the research, the author sought to answer several questions:

- What is known about school safety and security technology based on the current body of knowledge?
- Are there common themes, characteristics, data, or other evidence on school safety technology in the literature?
- What lessons, if any, are conveyed in the literature about the efficacy of school safety technology?
- What types of technology are currently in use, how do schools select technology, and what data exists about the effectiveness of those technologies?

The review considered the following areas:

- K-12 schools in the United States
- School safety overview, including definition and current data
- School safety technologies, including access controls, locks, cameras, communications and emergency notification systems and its effectiveness
- Selection and evaluation of technology, including risk assessment and other planning considerations
- Findings

Once completed, the literature review served as a foundation upon which other sections of the Comprehensive Report on School Safety Technology could be built.

13.1.1 METHODOLOGY

This literature review draws on available academic literature and other published sources to assess what is known about the use of technology to prevent acts of criminal violence in schools and advance and maintain a school's safety and security.

The literature search targeted three primary sources: journals, government reports [including research published by the National Institute of Justice (NIJ)], and professional and association publications (education, security, technology, and others). Secondary sources included news articles, conference proceedings, and vendor or corporate publications. The search strategy involved using a series of keywords, all of which were relevant to school and campus safety and security. Information for inclusion in the literature review was selected based on relevance to the previously discussed guiding questions and others posed by the research team.

More than 3,000,000 articles (popular media, scholarly publication, and others) have been written on school safety. To begin the process, 420 academic journal articles and 740 books and other media sources, including news media, having relevance to this review, were identified. This represents only a portion of the available literature. More than 200 journal articles and 300 books, professional magazines, and popular media articles (including articles and discussions in social media) were scanned. Of these, approximately 130 documents with a high degree of relevance were reviewed in detail. Attention was given to articles generated by practitioners, such as school administrators and security experts, in addition to the evidence generated by academics and researchers.

13.1.1.1 Limitation of the Literature Review Process

Some of the literature, particularly professional documents, addresses technology in the broader context of school safety and student, teacher, staff, and visitor well-being. Discussion about technology is embedded throughout the text but not addressed independently. For example, a study of 16,000 schools (Reference 314) showed that basic safety technology such as fire alarms and extinguishers, exterior lighting, door locks, and student lockers are in use consistently regardless of region or other demographics. Much of the literature on school safety technology goes beyond security and prevention of criminal acts and aberrant behavior. It encompasses fire prevention and response, healthcare, an array of environmental issues (e.g., air quality, hazardous materials, waste disposal, and pest management), ingress and egress to school facilities, vehicle and traffic control, and the relationship of technology and the school environment to academic achievement. Such literature, while highly relevant to school safety procedures, is outside the scope of the concept of school technology and mitigation of school violence.

Although literature specific to individual technologies was reviewed for each of the technology chapters, the results of that research are presented in the relevant technology chapter rather than this one.

A limited number of articles also combine Pre-K to grade 12 with college and university campuses in addressing security threats, needs, and solutions.

There is no national system for reporting the type of safety and security technology in a school or its effectiveness. Research on school safety technology has been inhibited by inconsistencies in the available data and information on planning, policy and regulation, types of technology in use, and methods of assessment.

Lastly, the literature on school safety technology tends to focus on the types of technology and people's perceptions of it rather than its efficacy. The need exists to expand the body of knowledge on the appropriateness or fit of school safety and security technology and its effectiveness over time. Measures of effectiveness, in addition to simple changes to statistics (e.g., increasing or decreasing number of incidents), need to be developed, standardized, and conveyed.

13.2 TYPES OF SCHOOLS

On any given day, public schools are among the largest organizations in urban, suburban, or rural jurisdictions or regions. Generally, when public schools are in session, they are some of the most densely populated locations in any community. For example, enrollment ranges from 2277 to 5858 students within the 1000 largest high schools in the United States (Reference 235).

There are more than 132,000 schools in approximately 14,000 school districts in the United States. Of these schools, 98,817 are public. There are approximately 54,876,000 students in the nation's K-12

schools (Reference 89). Schools employ approximately 3.1 million full-time equivalent teachers. One-third of the nation's public schools are rural, serving approximately 12 million students (References 234 and 321).

School systems are highly fragmented. They include large city and county systems, individual school districts within the same jurisdiction, independent school taxing districts, parochial schools (ranging from large diocesan systems to schools associated with a small religious institution or group), private schools (nonprofit and profit-making), and others. They are overseen by state agencies, independent boards, and other forms of governance.

Regardless of the type of governance, schools in most systems have a high degree of autonomy regarding decision making about school safety and security technology, but the tremendous variation between the organization, funding, social and legal environments of schools, school districts, and their communities makes general recommendations difficult to defend.

13.3 DEFINING SCHOOL SAFETY

While extreme or extraordinary acts of violence in schools such as mass casualty shootings remain rare, they have garnered international attention (Reference 116). The extreme consequences of these events evoke emotions similar to terrorist attacks. Thoughts and images of these events spark fear, and that fear can result in reactive decisions that may not be ideal (Reference 91). Incidents such as the heinous attacks at Sandy Hook Elementary in Newtown, CT, and in other locales (Moses Lake, WA; Pearl, MS; Paducah, KY; Jonesboro, AK; and Littleton, CO) come to the forefront in almost every conversation about school safety and have generated a societal belief that schools are becoming dangerous places (Reference 344).

13.3.1 CURRENT DATA ABOUT SCHOOL SAFETY

School safety and order are essential conditions for learning in all schools regardless of the environment, locale, or community demographics (Reference 77). Repeated crimes (serious and non-serious) disrupt the environment and impede learning. Safety and order in schools also may be disrupted by threat, fear, hate, revenge, disagreement, and other actions and behaviors that may not rise to the level of criminal acts.

Safety-related concerns in schools are far reaching and include issues such as theft, bullying, cyber-bullying, vandalism, threat, suicide, assault, trespassing, sexual assault and intimate partner violence, racial tension, hazing, crowd control at special events, transit and traffic safety (including safety on school buses), and more (Reference 171).

Although wellbeing in schools is difficult to measure, most indicators reinforce that school safety is increasing. Data show that criminal offenses committed by people who belong in schools as well as those from outside the school environment are infrequent and have declined in recent years. For example, since 1992 the rate of victimization for violent and nonviolent incidents in schools has declined from 181 incidents per 1000 students to 49 per 1000 (Reference 290).

The vast majority of the literature corroborates the conclusion that public and private schools are safe (Reference 270). Whether located in urban, suburban, rural, or tribal communities, the students, teachers, staff, and guests in schools experience few serious crimes. Nonetheless, the nature of aggression in schools continues to change. In a national survey of school administrators, premeditated

aggression among middle and high school students, as compared to reactive aggression, has tripled in the past 20 years (Reference 215).

Research indicates that teachers are particularly concerned about safety and security relevant to the needs of students who have disabilities. Students with developmental and other disabilities are disproportionately exposed to violence and other types of crime and inappropriate behavior and need specific interventions tailored to their unique needs (Reference 121). There are specialized types of safety and security technology in place in some schools to assist students who have special needs. These include collapsible wheelchairs kept in stairwells and lighted alarms for students with hearing impairments, but the literature on the application of technology to address violence against these students is limited (Reference 36).

Although the safety of students is a critical priority, safety technology and procedures also affect the safety of all occupants and visitors. Literature on violence against teachers and other employees in schools is limited, but some data indicate that on a per capita basis teachers are more likely to be threatened or assaulted than are students (References 96, 188, and 219).

13.3.2 WHAT IS A SAFE SCHOOL?

Research shows that a positive or negative perception of a safe school facility, combined with other environmental factors, impacts students behavior and learning (References 27 and 299). Some research shows that prevention practices in schools do not significantly reduce the likelihood of violent victimization or perceptions of risk, whereas other research states that security technology may reduce the probability of crime within the school environment (References 343 and 369).

The Department of Homeland Security recognizes school facilities as vulnerable sites (Reference 308). Among the factors that influence this vulnerability are open access to the school environment and freedom of movement within school boundaries. The degree to which school facilities should be open or secured remains a subject of debate among educators and law enforcement officials.

California's Proposition 8, The Victims' Bill of Rights, contains a safe-schools provision that states that all students and staff of primary, elementary, junior high, and senior high schools have the inalienable right to attend campuses that are safe, secure, and peaceful.

Within the current body of literature, finding a definition of a safe school that provides a clear and quantifiable understanding of what it should be is difficult. Reports, conference proceedings, news stories, and journal articles offer definitions of a safe school related to the documents' purpose to help frame the content. Definitions exist for terms such as *external environment*, *bus safety*, *weapons detection*, *targeted violence*, *classroom management*, and *zero tolerance*. But a universally accepted, practical definition of a *safe school* is elusive.

Many of the definitions describe a safe school in terms of an absence of negatives or in regard to a specific type of incident such as bullying. For example, one definition describes a safe school as one in which all stakeholders have come together to minimize the opportunity for bullying and other forms of violence (Reference 374). Others define a safe school in broad or evasive terms that do not easily drive actions, such as one in which the environment is conducive to learning.

According to the Center for the Study and Prevention of Violence at the University of Colorado at Boulder, a safe school is one that is prepared for emergencies, provides opportunities and guidance for students before and after school with programs and activities, and involves the whole community in

anticipating and preventing school problems. A safe school requires balancing physical security with a nurturing school climate, as well as developing effective school-community partnerships (Reference 57). There are numerous legal and ethical issues relevant to security technologies that are addressed independently of the literature that defines a safe school (References 286 and 379).

Research continues to be conducted on crime and violence in schools including a study on the role and value of school resource officers (SROs) (References 44 and 45). The body of research on crime and fear external to school facilities, including crime along routes of ingress and egress and the impact of crime in neighboring communities, is also growing.

With no standard definition of school safety, the research has often focused on the perception of safety by various audiences, including the students, the teachers and staff, and the general public. Differences in perceptions may influence decisions about the technology needed to address safety needs.

13.3.3 PERCEPTIONS OF SCHOOL SAFETY AND TECHNOLOGY

Although some literature cites the presence of security technology in schools as a source of increased fear, there is no conclusive evidence that it influences fear positively or negatively overall. There are other variables such as community poverty, type of school (e.g., public, private, or parochial), school climate, gang problems, and school density and enrollment that impact feelings of safety and security, fear, and victimization (Reference 272). Many of the nation's most serious attacks in schools have occurred in small towns and rural communities, changing long-held perceptions that crime and disorder are limited to urban schools (Reference 101).

13.3.3.1 Teacher and Staff Perceptions

A recent study conducted in an Ohio high school paralleled national survey responses that showed the vast majority of teachers and staff (94%) believe their school is a safe place to work. A smaller number (67%) perceive their school as sufficiently prepared for a major incident such as a shooting (Reference 284).

Generally, pre-service and less-experienced teachers expressed more concern about the possibility of a major criminal event such as an active attack occurring in their school and, particularly, about their ability to deal with the event. Experienced teachers expressed more concern about the general safety of their students and felt more confident about their ability to manage an incident. Emphasis needs to be placed on how teachers are made aware of and taught to use safety technology and other intervention tactics and to manage their own fear as well as that of others (Reference 384).

A 2013 survey of 10,661 educators in 50 states by the School Improvement Network found that:

- 91.6% of educators feel safe in school
- 94.5% of educators believe their students feel safe in school

In some cases perceptions about the value of school security technology have been challenged by study. For example, one study showed that although principals believe requiring students to wear school uniforms has a positive impact in preventing crime, the evidence shows the impact to be limited, at best (Reference 174). Another study also found the value of uniforms in preventing crime in schools questionable, although it did find uniforms worthwhile in improving general student behavior, keeping track of students on field trips, and identifying the presence of outsiders (References 38, 328, and 377). A perception of particular interest to this study is the apparent belief that technology is needed to

address school safety. And yet, the presence of adult supervision in hallways, rather than high-visibility technology, was identified as effective in reducing peer victimization by 26% according to one study (Reference 35).

13.3.3.2 Student Perceptions

There is little research on student input as to the use and placement of security technology or other safety-related practices in schools. The school climate often determines the extent to which students want to engage and share information about security concerns (Reference 43). A survey of youths in grades 9 through 12 conducted by the Centers for Disease Control and Prevention in 2014 presented the following findings:

- 8.1% reported being in a physical fight on school property in the 12 months before the survey.
- 7.1% reported that they did not go to school on one or more days in the 30 days before the survey because they felt unsafe at school or on their way to or from school.
- 5.2% reported carrying a weapon (gun, knife, or club) on school property on one or more days in the 30 days before the survey.
- 6.9% reported being threatened or injured with a weapon on school property one or more times in the 12 months before the survey.
- 19.6% reported being bullied on school property, and 14.8% reported being bullied electronically in the 12 months before the survey.

Despite the survey results about violence, students generally believe their schools to be safe and perceive that many of the security strategies in use in their schools are unnecessary (Reference 40).

A Canadian study on perceptions about bullying showed that students in elementary schools felt most vulnerable on the playground, in the schoolyard, and during recess. Secondary school students felt least secure in hallways, school cafeterias and lunchrooms, and during recess. However, there were no indicators that school officials use such information when making decisions about the type or placement of security technology (Reference 367).

Students tend to see value in the presence of school police officers and SROs. They also tend to believe that drug-sniffing dogs play a role in reducing the presence of illegal substances in school. Students perceived that, with the exception of the dogs, most security measures had little impact on the presence of drugs or guns in school.

In a study of 230 high school students, there was no consensus on the value of video surveillance cameras in preventing crime in schools (References 44 and 45). Student perception toward weapons detection technology (e.g., metal detectors) ranges from the belief that they unnecessarily cause increased fear of violence to a belief that their presence prevents students from carrying weapons to school (Reference 146). The security measure that students perceive has the least value is transparent (i.e., see-through) backpacks. Male students were significantly more likely than females to negatively evaluate the effectiveness of SROs, metal detectors, and other security measures (References 44 and 45).

Some of the literature cites concern that increased security in schools may have unintended negative consequences (Reference 310). The concern focuses on fear as the catalyst for changes in school security, rather than study or logic. It also focuses on types of visible security adopted by schools after Columbine and the positive and negative consequences of these measures. Schools that have not had

significant problems but seek to implement highly visible security technology may unnecessarily exacerbate student fear and concerns about crime (Reference 307).

Identifying what students believe about school safety and incorporating their input when deciding what technologies to implement could bring significant benefits to the overall effectiveness of those technologies.

13.4 SCHOOL SAFETY TECHNOLOGIES

Implementation of security-related technology is a component of a comprehensive safe school plan or initiative (Reference 16). For the technology to be effective, it must be considered as part of a comprehensive school safety initiative. According to William Modzeleski, former Associate Assistant Deputy Secretary U.S. Department of Education (DoED), “There is no one program, no silver bullet, so that you can get one program up and say...you are going to resolve violence.” (Reference 373) In 2013, nearly all students ages 12 to 18 reported that they had observed the use of at least one security measure at their schools (Reference 392).

Factors that contribute to school safety include the presence of a plan, policies and procedures, disciplinary practices, administrative and community support, faculty and student acceptance, the state of the environment (internal and external), staffing, and internal assessment. Community demographics, budget, and legislation also are contributing factors.

Although some of the literature references the importance of meeting the specific needs of each school, there is limited evidence-based information on how to conduct a technology assessment to determine those needs and identify the appropriate solution. Some schools that have very few problems or threats are well-equipped or over-equipped with safety and security technology, whereas other schools that have recurring crime and related needs have little or none of the needed safety and security technology.

13.4.1 TYPES OF AVAILABLE TECHNOLOGY

Innovative technologies for school safety and security are on the market worldwide. The spectrum ranges from traditional and basic technology such as locks and public address systems to more advanced equipment such as tracking tags that monitor the location of every student (Reference 63).

The literature review revealed a variety of types of safety technology available for use in schools which includes:

- “Intelligent” video (smart cameras)
- Classroom telephones (fixed and wireless)
- Communication and alert systems, ranging from use of social media to megaphones
- Data security and cybersecurity systems
- Electronic access and lock-and-key systems
- Generators
- Global positioning system and other tracking devices (on school buses, implanted in valuable equipment)
- Identification card and swipe systems
- Information recording and storage
- Interoperable communications (shared radio, text, video, and other data)
- Lighting (including emergency and backup lighting)

- Online communication monitoring
- Protected storage
- Rapid-access databases
- School web site security information
- Standard and panic alarms
- Surveillance cameras (fixed, moving, black and white, color, high definition)
- Visitor badging and control
- Weapons detection

One way to consider safety technology in schools is by taking into account the impact it is intended to have on the incident. Some technologies help to prevent a crime from happening, some are intended to minimize the effects of violence by adding a layer of protection, whereas others are critical during an active incident.

Lastly, broad categories of overall purpose may be used to consider technologies. In general, school technologies address three categories of purpose: crime prevention (e.g., physical security technologies, social media monitoring), collecting and transmitting information, and incident management. Some technology types serve multiple purposes.

Generally, school safety technologies can be discussed by considering the function they are intended to provide.

13.4.1.1 Access Control and Crime Prevention

Almost all schools employ the basic technologies to control access to schools and deter crime through use of door locks, lighting, public address systems, and the marking of school property. Burglar alarm systems, controlled access, and posted signs are used in most schools. Duress alarms are installed in a majority of classrooms. Another commonly used security-related technology is fencing. Outdoor perimeter security sensors have been used as a security measure for 40 years (Reference 150). Modern perimeter sensors are wireless and behavior-driven and involve live-feed video surveillance.

There also is special security technology in place to support school bus safety, areas of ingress and egress, and special events (sporting events, community programs and meetings, voting, graduation). The National Center for Education Statistics report cited that in the 2011–2012 school year, almost 90% of public school controlled access by monitoring or locking doors during school hours (Reference 324). A similar percentage used cameras to monitor the school perimeter and hallways and locked and monitored gates and storage areas.

13.4.1.2 Surveillance

An increasing number of local police agencies are linking directly to live video feeds from schools. Videos are conveyed via wireless technology directly to the computers in police officers' vehicles. This technology is important to those schools that do not have SROs onsite and therefore depend on local patrol officers, deputies, and troopers to respond to incidents. For example, there are 128 cameras in use in five schools in the Franklin Regional School District in Pennsylvania. Live feed from each camera can be sent directly to officers in area police departments. The video feeds have the potential to assist the initial responding officer, deputy, or trooper in planning a course of action prior to arrival, protecting students and others, and managing the response of backup officers and other emergency services personnel (Reference 274).

The majority of schools in the United States do not have full-time SROs assigned to them. They rely on local or state police officers for support, especially in time of crisis. Although calls about crime and disorder generate a significant percentage of police involvement in schools, officers report increasing participation in other roles such as traffic control, sports events, class presentations; few details are available on the effects on school safety (Reference 182). There is limited research on the role that local officers play in securing the safe travel of students and others during periods of ingress and egress, and there even less information about the role these officers may have in reducing fear of victimization and preventing incidents within schools. It is incumbent on both school and police officials to educate area officers to each school's prevention and response protocols and technologies.

13.4.1.3 Threat Detection

Approximately 11% of schools conduct random sweeps to check for weapons, 9.4% reported using alcohol detection devices, and 6.8% required random drug testing for students. Despite the common perception that most schools use metal detectors, only a small percentage (one study estimates fewer than 2%) require students to pass through them on a daily basis. Less than 1% use scanning devices to check contents of school bags (Reference 75).

One of the areas of rapid advancement in security technology in schools is the use of Internet filtering and other protective measures to prevent harm from bullying and other crimes, intrusion, and inappropriate access to information via the Internet (Reference 370). The Children's Internet Protection Act (CIPA) requires schools that receive funds from the Federal E-Rate program to implement web-filtering technology to prevent users from viewing objectionable material while they are using the institution's computers. The literature is extensive on the need for and implementation of protections against computer-based crime. The literature on the efficacy of efforts to protect students from web-based accessibility to sites and people that could result in crime is far less extensive.

13.4.1.4 Threat Assessment

It is not enough to know that a threat exists. Schools must determine the risk of actual harm associated with a threat and initiate an appropriate response. In 1998, the National School Safety Center (NSSC) published characteristics of youth who caused school-associated violent deaths (Reference 330).

The following is a sampling of the characteristics on the NSSC list:

- Has a history of tantrums and uncontrollable angry outbursts
- Characteristically resorts to name calling, cursing, or abusive language
- Habitually makes violent threats when angry
- Has previously brought a weapon to school
- Has a background of serious disciplinary problems at school and in the community
- Has a background of drug, alcohol, or other substance abuse or dependency
- Is on the fringe of his/her peer group with few or no close friends
- Is preoccupied with weapons, explosives, or other incendiary devices
- Has previously been truant, suspended, or expelled from school
- Has witnessed or been a victim of abuse or neglect in the home
- Has been bullied and/or bullies or intimidates peers or younger children
- Prefers reading materials dealing with violent themes, rituals, and abuse
- Reflects anger, frustration, and the dark side of life in school essays or writing projects
- Is often depressed and/or has significant mood swings

- Has threatened or attempted suicide

The list was designed to serve as a guide for administrators, teachers, and support staff, but reading it indicates how difficult it would be to proactively identify such traits and isolate true threats from the wide group of people likely to have expressed some subset of such an expansive list.

13.4.1.5 Communication

An area of rapid advancement in schools is the use of wireless technology, especially cell phones, to improve communication in various types of crises to include crime, fire, and weather emergencies. Some school systems issue mobile phones to all teachers and other staff. Large schools with expansive facilities and schools that make use of portable classrooms have found wireless communication technology to be essential components of their security efforts. To take advantage of their existing telecommunications infrastructure, schools are inexpensively adding wireless voice capabilities to their existing wireless local area networks (Reference 142).

13.4.1.6 Integrated Technologies and Situational Awareness

Although advances in school technology have evolved and continue to evolve, the integration of the technology is a more recent area of concern and development. Integrated technology—physical security, software, internal communications and monitoring, and shared information among agencies—will continue to be a primary area for development and expansion in the future. Well-planned integrated systems, which have been implemented in some schools, appear cost effective. Development of such systems and technology to integrate existing systems will be an area of innovation in the coming years (Reference 119).

The literature shows a significant interest in integrating systems and the data generated to enhance understanding of the school environment and provide real-time situational awareness of threats. The types of technology often integrated with other systems include software, alarm systems, video cameras (with direct live feed to responding public safety personnel), backup generators, emergency lighting (exits and hallways), social media, public address systems, and direct and remote-controlled classroom door locks.

Alabama is one state that requires local boards of education to adopt a comprehensive school safety plan for each school under their authority. The plan must include a protocol and procedures for addressing threats to the safety of school property, students, employees, and administrators and for responding to any emergencies that compromise the safety of school property, students, and employees. A statewide initiative funded by the Alabama Department of Homeland Security creates a “digital footprint” of schools that provides detailed information, photos, maps, and other information to first responders in real time. The effort is part of a state mandate to map all K-12 schools. Alabama is one of the first states in the nation to adopt the system, entitled Virtual Alabama School Safety System (VAS3), which is based on geographic information system (GIS) technology and a front-end Google Maps interface. The system currently provides 51 categories of information on any given school and is being expanded (Reference 204).

13.4.1.7 Additional Types of Technology

Of the types of security technology in use in schools, biometrics is among the least used. Biometrics is automated recognition based on an individual’s physiological or behavioral characteristics that are unique and almost impossible to imitate such as voice, signature, face, iris, or retina (Reference 316). It

is a recently emerging tool and is discussed as an advanced means for controlling access and entry (Reference 207). The application of biometrics in schools remains relatively immature (Reference 70).

13.4.2 WHAT TECHNOLOGY IS IN USE

Most public schools have become high-security environments (Reference 40). A study of security technology in U.S. schools using information from Common Core of Data (90,000 schools) found that 98.6% of schools reported using security technology (Reference 75). The remaining 1.4% likely use locks, door alarms, signage, and other basics, but administrators who responded to the survey likely did not recognize them as technology worth reporting.

Generally, the use of security measures is higher among public schools than in private schools. For example, 64% of public schools reported using cameras to monitor the schools versus 41% of private schools. Public schools also made greater use of identification badges, requiring transparent book bags or banning book bags, employing metal and weapon detectors, and conducting random sweeps for contraband (including use of K-9 dogs). Private schools were more likely to enforce strict dress codes or require students to wear uniforms (Reference 290).

A study of 16,000 schools showed that basic security measures such as exterior lighting, door locks, and student lockers remain the most widely used and trusted means of prevention (Reference 314).

A review of state guidelines showed the most common types of safety equipment cited:

- Access to electronic databases
- Camera housings
- Card scanners, identification systems, and biometrics
- Duress alarms
- Entry control and remote access technologies
- Fencing
- Lighting
- Lockers
- Metal detectors
- Signage
- Uniforms and dress codes
- Video cameras
- Video recording

The available literature rarely specifies the types of safety and security technology actually used in schools and precise details on characteristics of the technology and manufacturer names often are absent. For example, in a review of 20 randomly selected scholarly articles on metal or weapon detectors in schools, none referenced the brand name of the product(s). Half of the articles defined the use of stationary or handheld devices and none referenced in-ground or “invisible” detection devices. Similar details were lacking concerning emergency alert systems, integrated systems, high-resolution cameras, and other technology.

The use of school safety technology varies significantly by community and geographic region. Schools in the South reported higher levels of use of security technology than those in other parts of the United States. Larger schools located in urban areas and secondary schools reported greater use of security technology than smaller schools and those in suburban and rural areas. Perceptions of school crime

influenced the extent and type of school security technology, as did perceptions of crime in the neighborhoods that surround the school (Reference 75).

13.5 SAFETY TECHNOLOGY SELECTION AND EVALUATION

Since the shooting at Columbine High School in 1999, changes in security measures have changed the social climate of schools (Reference 40). The move to advance school safety and security technology began shortly after Columbine, with rapid and expanded use of existing devices and a somewhat slower movement toward design of new equipment and software (Reference 31). New security technology, laws, disciplinary policies, SRO programs, and other initiatives occurred in the years that followed, but minimal attention was given to the study of stakeholders' perceptions of their value.

There is little consistency in the literature that corroborates the conclusion that safety and security technology in use in schools is a result of a prior comprehensive assessment of risk or threat. According to the National Clearinghouse for Educational Facilities (NCEF) (Reference 239):

School safety can be enhanced by the appropriate use of security technologies such as alarm systems, smart cards, and surveillance equipment. Technology can be expensive, however, and require ongoing maintenance, repair, and frequent upgrading by specialized employees or service contractors. It can be oversold or mismatched to the problems being addressed. In some cases, it may reinforce fear and undermine the social ecology of the school. For these reasons, you carefully think through the costs and benefits of each technology, closely evaluate all sales pitches, and talk to as many vendors as possible before making a decision.

A review of literature by RAND Corporation in 2001 confirmed that schools had been using technology and tactics such as metal detectors, police officers, security guards, rules and regulations regarding student conduct and dress, profiling of potentially violent students, anti-bullying, and counseling and mediation for 15 years. The RAND review showed that, at the time, few of these tactics had been evaluated and fewer were deemed effective or promising (Reference 176). Other research shows that such technologies and tactics have been in use in schools for more than 30 years, beginning before Columbine and other high profile events (Reference 226). Although the use of security technology in schools has been a staple for years, school safety continues to grow more complex.

13.5.1 THE DECISION-MAKING PROCESS

...educators are often left in the precarious position of impending liability in either negligence, for failure to prevent violence, or civil rights tort, when they implement procedures and policies that are meant to bring order to school environments.
(Reference 154)

There is little research on the factors that lead schools to adopt security technology and other measures such as policies, personnel practices, and SROs (Reference 227). There is no research on the extent or quality of involvement of school officials, police officials, and other practitioners in the adoption of legislation or policy relevant to school security measures.

Unlike fire prevention technology that generally is regulated by state and local codes, school technology related to crime prevention and intervention is largely unregulated (Reference 126). Responsibility for controlling technology such as video cameras, entry control devices, and alarms is assumed by state, regional, and local school systems and, in some cases, individual schools.

Published state standards or benchmarks on specific technology brands, vendors, and quality of products are rare. Most school systems require vendors to register and meet certain criteria to compete for contracts. Schools in these systems have access to approved vendor lists. In some systems such as the McKinney Independent School District in Texas, the vendor list is all inclusive and does not distinguish providers of safety and security technology. Systems such as the Ohio DoED provide guidelines to schools on how to select vendors. Several state guidelines provide an anticipated range of costs to guide school administrators in planning.

In 2000, Virginia created the Virginia Center for School Safety to review mandatory school safety audits and provide training and technical assistance to school districts. The Virginia School Safety Center is primarily funded by Federal grants, although the state contributes some funding through its Department of Criminal Justice Services, of which the Center is a part. The Center also supports application of the Virginia Model for Threat Assessment (Reference 76).

An NIJ-funded study on school safety technology conducted in 1999 involved a survey of school districts in 15 states. The research resulted in a report by Green (Reference 139) that addressed issues such as the funding of technology and offered a range of costs for specific items such as video surveillance, weapons detection devices, entry controls, and alarms. In addition to addressing capital investments, the report discussed site modification and the need for staffing, training, and equipment maintenance and repair.

The NIJ-sponsored survey provided guidelines to aid school officials in assessing vulnerabilities and provided information on the applicability of security-related technology. Green's report (Reference 139) is one of the few documents that referenced the appropriateness and costs associated with implementation and maintenance. It addressed video surveillance, weapons detection devices (walk-through and handheld metal detectors and x-ray baggage scanners), entry controls, and alarms.

Although it is deemed essential that school safety and security efforts fit the individual needs of each school, many simply follow regional or national trends. There is limited data that show a relationship between the technologies in place and needs assessments conducted by individual schools (Reference 16).

The NSSC states the following (Reference 172):

A school safety assessment is a strategic evaluation and planning tool used to determine the extent of... school safety problem(s). An assessment could address gangs, weapons in school, drug or alcohol abuse, schoolyard bullying, site evaluation of facilities including buildings and landscaping, policies and procedures, compliance with local and state laws, community support, parent attitudes, student attitudes and motivation, or other emerging school climate trends.

13.5.2 IDENTIFYING THE THREAT

The diversity of the design and use of schools complicates selecting safety technology. Schools must deny access to unauthorized people, while allowing entry by staff, student, parents and authorized visitors. School facilities also may be open to the public for sports, performing arts, and community events. A typical school has a highly diverse physical environment, including:

- Areas with open access (e.g., corridors, elevators, stairwells, classrooms, libraries, cafeterias, auditoriums, gymnasiums)

- Areas with limited access (e.g., offices, faculty lounges, custodial rooms, utility rooms, and food preparation areas, laboratories and shops)
- Areas where privacy is expected (e.g., restrooms, locker rooms, offices, health rooms)
- External spaces (e.g., athletic fields, parking lots, recess areas, school buses, portable classrooms)

These competing needs vastly complicate efforts to implement safety technology. The NCEF, a component of the National Institute of Building Sciences, prepared and published a guideline for assessing these diverse areas (Reference 239). Since preparing the list, the NCEF shut down due to lack of funding. However, most resources indicate that the best way to select safety technology is to first determine what threats need to be mitigated and then determine the best solution.

13.5.2.1 Risk Assessment and Planning Tools

There is a large volume of general literature on risk assessment and planning tools for schools. Numerous articles call for all schools to conduct risk assessments and a large number of online sites offer risk assessment toolkits. One of the best general guides to such assessments is *A Guide to School Vulnerability Assessments*, published by the U.S. Department of Education, Office of Safe and Drug-Free Schools in 2008 (Reference 356).

Major organizations, Federal agencies, and state school systems provide risk assessment information, guidelines, and tools. While some tools primarily target assessing high risk and potentially violent behavior, almost all give attention to facilities and technology. The following is a small sample of the information available:

- Eastern Kentucky University – School Critical Incident and Risk Assessment
- Florida DoED – Safe Schools Design Guidelines: Strategies to Enhance Security and Reduce Violence
- Madison Metropolitan School District – Violence Risk Assessment Procedures and Tools
- National Clearinghouse for Educational Facilities – Mitigating Hazards in School Facilities
- National Institute of Standards and Technology – Risk Management Framework
- New Jersey DoED – School Safety and Security Plan Review Checklist
- North Carolina Department of Public Instruction – Safe Schools Facilities Planner
- Ontario Ministry of Education – Caring and Safe Schools in Ontario
- Texas School Safety Center – Campus Safety and Security Audit Toolkit
- U.S. DoED – Threat Assessment in Schools
- University of Colorado at Boulder – Safe Communities-Safe Schools: Pre-planning Assessment Checklists
- Virginia DoED – School Safety Audit Protocol

The scholarly literature is extensive in addressing the need for risk assessment in schools and generally cites the components of risk assessment tools and processes; however, few articles evaluate these tools and processes.

13.5.3 QUANTIFYING EFFECTIVENESS OF TECHNOLOGIES

Once the threats and potential consequences have been identified, the best technologies are likely to be those that are most effective at mitigating high priority risks and protecting against high priority threats. There is an extensive body of literature on school safety and the types of technology being used to

advance security in schools. The literature is slight, however, on the effectiveness of the technology and why schools or school systems choose specific technologies. Popular and professional media along with scholarly literature foster ongoing debate over the relevance and use of some of the technology in schools.

The debate over the effectiveness, including cost effectiveness, of safety and security technology suited for specific schools and systems continues among school administrators, teachers, parents, and facilities designers (Reference 177). For example, headlines from one website included: “Are schools wasting limited money on questionable security vendor products?” and “Plan for laminate window film raises questions about school security priorities, ‘expert’ credibility.” (Reference 248).

The volume and types of security and prevention efforts in some schools are considerable. There is limited and conflicting evidence on the short- and long-term effectiveness of school safety technology. Some of the literature attests to the success of school safety efforts based on simple statistics and an absence of negatives without identifying or substantiating the variables that may have caused that statistical change or absence of negative events.

Many of the activities that schools undertake to promote safety and prevent problems, including use of technology, have not been evaluated. Information available in reports and articles on the type and quantity of technology in use in schools is based on self-reporting (Reference 146). The literature is sparse on the use of independent inspections or other means to verify the self-reported information. The number of safety-related policies, procedures, and devices in place in these schools raises concern about the ability to manage and assess them effectively and realize benefit from their application (Reference 137).

Although school principals have some influence on use of technology, they cannot compel teachers, staff, and others to use it in times of crisis. Teachers, administrators, staff, students, and volunteers, along with others who use school facilities (such as coaches and neighborhood leaders), need to be well-versed in use of technology prior to an incident (References 152 and 264). Training and comfort in using the technology are paramount (Reference 223). Accessibility and maintenance and testing are equally important.

Despite the movement to increase security measures in schools, including technology, the effectiveness of these measures in preventing events ranging from student misbehavior to criminal violence remains largely unexamined. Past reviews of the literature show that there is a lack of information on the evaluation of the effectiveness of school security in general, including technology (Reference 2).

13.5.4 RESOURCES FOR DECISION-MAKERS

13.5.4.1 State Recommended School Security Guides

There is no national clearinghouse or center serving as an “honest broker” to test or recommend specific technologies or vendors to schools. As a result, many school officials rely on vendor-sponsored research, word of mouth, advice from police or security personnel, internal review, or grant funding criteria for making procurement decisions. Current evidence is limited on the success or cost effectiveness of technology in schools to prevent and mitigate crime, disorder, and catastrophic events (Reference 157).

Since its publication in 1999, the NIJ-sponsored report, *The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies*, has been used by states to provide assistance to schools and has been incorporated in or modified as part of state

guidelines (Reference 208). Guidelines in several states are provided for the purpose of assisting schools in applying for state grants to fund safety and security technology. In several states, guidelines for schools are provided in response to legislated mandate.

State guidelines are referenced in much of the literature. For the purpose of this review, guidelines from several states in different areas of the United States were reviewed in detail. The literature indicates that each of the reviewed states is directed to assist local, county, and regional school systems. However, state guidelines focus on policy, prevention, and response and are provided as recommendations rather than standards.

Most of the state guidelines and checklists on school safety are comprehensive and incorporate broad definitions of safety. Almost all address fire, emergency management, and health, with some going into detail on tornadoes, hurricanes, earthquakes, school bus crashes, and hazardous materials, in addition to intruders, theft, weapons, and other crime-related threats. Two of the state guidelines evaluated reflect the need for schools to comply with Federal or state Occupational Safety and Health Administration (OSHA) regulations, but most states seem to address OSHA issues in a separate document (Reference 246).

In addition, they commonly focus on a wide range of security-related impacts (prevention, protection, mitigation, response, and recovery) and provide varying degrees of information on types of equipment. Some of the state documents, such as the “Minnesota Comprehensive School Safety Guide” provided to schools by the Minnesota Department of Public Safety in 2011, address specific areas of the school such as classrooms, the cafeteria, the gymnasium, parking lots, etc., and consider both physical and behavioral aspects of safety and security.

13.5.4.2 Influence of Law, Policy, and Regulation on Selection

Schools often have established policies and regulations and have worked with legislators to pass laws (local and state) to guide the use of technology such as video cameras and closed-circuit television (Reference 171). Policy, regulation, and laws also have been used to empower school authorities to deal with issues such as bullying, racism, student misbehavior, trespass, and carrying weapons on school property.

A study of 450 bills related to school safety published in 2013 by *Education Week* showed that most of the proposed legislation dealt with emergency planning, police in schools, and school climate. Of the 450 bills reviewed, 75 focused primarily on building safety upgrades. A common topic across the legislation was managing (preventing, controlling access, allowing) weapons (Reference 100). Schools across the United States have had to modify law and policy to allow SROs and, in a smaller number of systems, teachers and school administrators to carry weapons on school property. Other legislation passed or considered in schools nationwide includes passing gun control laws and using vigorous Federal and local enforcement of existing gun control laws; imposing civil or criminal liability on parents for their children’s violent behavior; establishing specialized courts and prosecution strategies for handling juveniles charged with weapons offenses; imposing stricter enforcement of school disciplinary codes; reforming the Individuals with Disabilities Education Act; and considering alternative schools in which to place students charged with weapons violations (Reference 285).

Policies, regulations, and laws supporting traffic control and travel to and from school are common across school districts and are growing steadily as a result of Safe Routes to Schools programs (Reference 94). Laws associated with these programs govern basic technological measures such as cross walks, bike paths, vehicle speed, and traffic control devices. Laws and regulations governing use of

driveways, turning bays, and stop zones at schools and proper use of these systems have been shown to reduce injury (Reference 68).

Laws and regulations related to school bus technology have proven effective in preventing and responding to crime and misbehavior, including traffic violations. Use of live-streaming video technology has led to the ID of vehicles that pass stopped school buses using all signals. The videos can be sent to law enforcement agencies rapidly for immediate enforcement efforts, can be used later to determine whether charges should be placed, and can be presented as evidence in court (Reference 202).

13.5.4.3 Influence of Funding Legislation on Selection

One of the complexities in advancing school safety and security technology is funding. Federal, state, and school system grants supported much of the post-Columbine security purchases. Implementation of advanced school safety and security technology declined with the economic downturn in 2008. In the years that followed, schools could no longer sustain their previous budgets (Reference 292). Some declined grants, knowing that the money was unavailable to maintain the equipment beyond conclusion of the grant. There is continued debate among educators, facilities designers, political leaders, law enforcement personnel, and others about the cost effectiveness of security technology.

The scholarly literature on expenditures on school safety and security technology provides little insight into cost by type of equipment. Little is known about expenditures on security technology in parochial, private, and charter schools (Reference 82). Data on school safety expenditures in the professional and popular media primarily is local and anecdotal (Reference 83). Few schools have the funding to move quickly from limited or no physical security to full-scale implementation of closed-circuit television, sophisticated entry devices, and other advanced systems. Some schools lack the funds to purchase cost-effective and widely accepted security tools such as ID card readers (Reference 124).

According to the Education Commission of the States, state legislatures throughout the United States have mandated or provided for safety and security technology as a component of school construction funding. This applies to new construction and enhancement of existing facilities. In 2009, the National Association of State Boards of Education (NASBE) prepared a summary of state legislation related to school safety. The following subsections provide brief examples of how state legislation could impact the selection of school safety technology.

13.5.4.3.1 *California*

California law authorizes school districts receiving aid for new school construction through state bond initiatives to use grants for, among other things, “equipment, including telecommunication equipment to increase school security.” In addition, districts may use state aid for school building improvements to pay for “furniture or equipment designed to increase school security.”

13.5.4.3.2 *Massachusetts*

Regulations adopted by the Massachusetts School Building Authority require school districts seeking state aid for school construction to submit a Design and Educational Program for each construction project and to include a description of the “overall security and the security measures taken to safeguard the facility and its occupants.”

13.5.4.3.3 Mississippi

The Mississippi legislature established a School Safety Grant Program in 2001, requiring the State DoED to administer the grant using only existing staff and resources. School districts adopt mandatory safety plans and then receive support to finance metal detectors, video surveillance cameras, communications, and monitoring equipment. Most funding for local school security is provided through Federal grants to the state.

13.5.4.3.4 New York

New York school districts apply for competitive school safety grants through the Omnibus School Violence Prevention grant program. Funding through the program supplies metal detectors, intercom and other intra-school communication devices, and other devices to increase school security and the safety of school personnel and students. New York law authorizes the education commissioner to provide school districts with additional building aid for approved purchases of metal detectors, security cameras, electrically operated partitions, and other security devices. State statute requires the education commissioner to annually prescribe a cost allowance for specific devices as part of New York's regular school facility funding.

13.5.4.4 Other Considerations Related to the Technology

Among the most notable technology trends are the need for a higher level of maintenance and increased monitoring of system use and capabilities (Reference 136) and the following:

- Cloud-based systems and services, wireless devices and connection of security systems to mobile devices (mobile phones and tablets)
- Integrated hardware and software (often unique to the vendor's product) and operational intelligence gathering integrating data from disparate systems
- Enhanced imaging and high-resolution cameras
- Ease of use and more energy efficient security technology

Table 13-1 summarizes the findings put forth in the 1999 NIJ report (Reference 10).

Table 13-1 Security Technology

	Pros	Cons
Video cameras	<ul style="list-style-type: none"> • Good deterrence for outsiders who do not belong on campus, especially when used in conjunction with warning signs. • Strong evidence is preserved on tape. • Less costly than human monitors. • Good documentation for liability claims. 	<ul style="list-style-type: none"> • The systems are expensive and can be logistically difficult to install. • Choosing the correct camera requires some technical knowledge. • Cameras can be stolen or vandalized. • Ongoing maintenance and operational support are required. • Some communities or individuals may challenge their legality. • Insiders can circumvent the system. • Students may move misbehavior to different parts of the school or campus.

Table 13-1 Security Technology (Continued)

	Pros	Cons
Metal detectors	<ul style="list-style-type: none"> • Detectors work very well. They are a mature technology and can accurately detect most firearms and knives. • Handheld detectors are affordable. 	<ul style="list-style-type: none"> • Detectors are only as good as their operators. • They are usually not effective when used on purses, book bags, or suitcases. • Walk-through detectors require more space than most schools have available. • Walk-through detectors usually require the additional use of handheld scanners for those who trigger the alarm. • The screenings are slow. • Devices cannot discriminate between an actual weapon and a benign piece of metal.
X-ray baggage scanners	<ul style="list-style-type: none"> • The systems are generally safe and effective in screening baggage for weapons. • They can generally scan between 10 and 20 items per minute. 	<ul style="list-style-type: none"> • They require well-trained and motivated operators. • They require substantial space.
Fences	<ul style="list-style-type: none"> • Defines property boundaries. • Forces intruders to consciously trespass and use a ladder or wire clippers to enter. • Keeps out casual strangers wandering onto school grounds. 	<ul style="list-style-type: none"> • Fences can be ugly. • Fences are expensive.
Coded ID cards or badges	<ul style="list-style-type: none"> • No manpower involved. • Technology is mature. • Cards can be switched off when lost or stolen. • Generally tamperproof. 	<ul style="list-style-type: none"> • No way to determine that only a single person is entering. • Cards can be lent out. • Card-swipe readers are subject to vandalism. • Card readers require maintenance. • Regular updating of authorized personnel database is essential.
ID card plus personal identification number (PIN)	<ul style="list-style-type: none"> • PIN and ID can be turned off when no longer valid. • Stolen ID card is not enough to gain entry. • Database automatically updates when ID is read and PIN entered. 	<ul style="list-style-type: none"> • More administrative effort is required. • Authorized people can let unauthorized people in. • Users can forget their PINs or lend them out. • Keypads can malfunction or be vandalized.

Table 13-1 Security Technology (Continued)

	Pros	Cons
Biometric identifiers	<ul style="list-style-type: none"> • This form of ID cannot be lent to someone else. • ID can be deleted when person is no longer authorized. • Nothing for a user to forget. 	<ul style="list-style-type: none"> • Not all systems are user friendly. • It is possible for authorized people to let unauthorized people in. • Sometimes the technologies malfunction and falsely reject an authorized person. • Devices are subject to vandalism. • They take longer to use than a card reader or keypad.

13.6 FINDINGS

While application of safety and security technology in schools is not new, headline-generated fears, fiscal issues, and advancements in technology have made the issue increasingly complex. The literature is sparse on how and why technology is selected and employed in schools (assessing need) and its influence on violence and other crimes (evaluation and impact). There is minimal literature on brands, vendors, or the advantages and disadvantages of specific technologies.

Much of the literature focuses on physical security technologies such as access controls, locks, surveillance cameras, and emergency notification systems. It also addresses technologies that facilitate exchange of information among schools, law enforcement agencies, and mental health providers to identify and mitigate threats. The types of technology schools use are expanding rapidly and include social media monitoring, behavior-triggered cameras, and biometrics. The literature tends to address implementation of security-related technology without connection to comprehensive safe school plans or initiatives, or other indicators of appropriateness of “fit.”

Technology has its limitations in identifying potentially violent offenders within the school. Characteristics of violent offenders in schools identified by NSSC show that intervention by administrators, teachers, and staff is more likely to be effective in identifying students at risk of committing an offense than most forms of technology.

Selection of school safety and security technology is often made at the individual school level by principals. Some choose from a dictated or recommended list of vendors provided by the system or state department of education, whereas others must identify providers on their own. In some cases, school architects are including security protection in new school plans.

There is no national system for collecting data on the type of security technology in schools, little information available on the efficacy of the technology, and no national database on school safety and security technology. Much of the information that is known about the volume and type of technology in use in schools nationwide is based on self-reporting or targeted research. Data may be recorded at the state, local, or system level. There is no center, organization, or agency that provides rapid access to state databases. Responsibility for controlling technology is assumed by state, regional, and local school systems and, often, individual schools. Research on school safety technology has been inhibited by inconsistencies in the available data and lack of information on planning, policy and regulation, types of technology, and methods of assessment.

Much more needs to be done to collect, analyze, and disseminate national and regional data on school safety and security technology. Focus of future research should be on types of technology, rationale for choosing specific types of technology, and vendors. More data are needed on the relevance of security technology to the needs of specific schools and how the needs were determined. More study is needed on the efficacy of the technology and its impact on prevention of and response to violence and other crimes.

The National Alliance for Safe Schools notes that schools have become a major and growing market for the security industry. The security industry recognizes that fear of violence and concern about liability cause school administrators to purchase security technology (Reference 56).

13.6.1 SCHOOL SAFETY

Little is known about why the systems, districts, and independent schools adopt specific approaches to school safety (Reference 283). There is minimal information available on the evidence or analysis processes applied to decision making about school safety and security technology. There is little information in the literature on the technology choices available to school administrators at the time when they made decisions to purchase or apply specific safety and security technology. There is little information in the literature on how many, if any, alternatives were available to school administrators when they made safety technology decisions.

Some school systems rely on national data, trends, and model programs to make determinations about technology with less emphasis on local analysis (Reference 16). Information sought by administrators in considering which school safety and security technology to select include cost-benefit analysis; review of the technology capabilities, strengths, and potential weaknesses; integration with existing systems; and potential for and ease of expansion (Reference 301). Again, it is unknown to what extent these considerations are applied.

13.6.2 SUMMARY

The literature review provides a brief snapshot of safety and security technology in K–12 schools. Although the literature has produced inconsistent findings, it was useful in meeting its intended purpose of providing a baseline perspective on school safety technology within the constraints of the methodology.

A vast number of scholarly articles have been published on the subject of technology related to ensuring the safety of schools. The literature on some aspects of school safety technology is extensive, focusing primarily on types of technology, from alarms to cameras, and people's perceptions of the technology. The professional literature and articles in the news media, on the Internet, and through social media is even more extensive. Despite the amount of research and published information, important questions about school safety and security technology remain unanswered.

This page intentionally left blank.

Chapter 14. INTERNATIONAL SCHOOL SAFETY TECHNOLOGY REVIEW

Sheldon F. Greenberg, PhD

14.1 INTRODUCTION

Preventing and managing violence in schools is a shared goal across most nations around the world, but the scope of prevention and security initiatives and data on the types of technology used and assessment of the applications vary greatly (References 46 and 291). To provide perspective and comparison to the study of school security technology in the United States, the author sought to identify school security methods and, in particular, technology-based approaches used worldwide.

Long before school violence consumed national and international headlines following the shooting incident at Columbine High School in 1999, school violence was a global issue. Violence and the threat of violence has affected and continues to affect communities in almost every nation in the world (Reference 5). Nations with cultures as diverse as Japan, Jordan, Brazil, Norway, Israel, Malaysia, the United States, and Ethiopia have been affected by incidents that have sparked national alarm about school violence. These incidents include gun violence in the United States, decapitations in Japan, hangings in Norway, and group stabbings in Israel.

Violence against students in schools affects approximately 1 million children worldwide every day. In response, Plan International implemented the Learn Without Fear Campaign in 2008 to reduce violence in schools. Working in 48 countries globally, with a special focus on Africa, Asia, and Latin America, the campaign's influence has led to legislative changes, training of teachers, and use of social media to communicate with students and the community (Reference 198).

Although research and literature on international school violence is growing, it is limited to several perspectives. These include compilation of statistical data on types of crime and attack, victim populations, and national or regional policy. International studies allow for comparison of incidents, causes, and country-specific needs (Reference 313). The literature on use of security technology and its outcomes, particularly in developing and underdeveloped nations, is slight. Much of the information available on school violence and school security technology is based on media reports, local and regional data collection, and anecdotal information.

The Global Coalition to Protect Education from Attack estimates that thousands of targeted attacks on schools have occurred worldwide since 2009. The majority of these attacks involved bombing and shelling, homicide and aggravated assault, rape and sexual assault, and kidnapping and abduction. In some nations, schools were, and continue to be, overtaken by armed groups (government and non-state) for use as bases of operation and detention centers (Reference 289).

In 2004, a terrorist attack killed hundreds of students, teachers, and parents in a school in Russia. This incident, along with the shooting at Columbine High School and other active shooter attacks occurring in the same period, focused much of the world's attention on preventing and mitigating large-scale attacks on schools by extremists and external forces.

Because many of the headline-grabbing attacks occurring around the world were committed by external forces, focus on weapons detection and emergency response—including military response—took precedence over addressing more prevalent types of internal violence (e.g., student on student, student on teacher, teacher on student) and surrounding community violence (e.g., drug and gang related) affecting schools (Reference 92).

The structure of schools across different nations varies considerably, and these variances affect the approach to and support for violence prevention and intervention. Significant variation exists in educational standards for students and teachers, quality of teaching, teacher support, and infrastructure among developed, developing, and underdeveloped nations. In addition, there is a diverse range of commitment to safety and security and protecting students and teachers from disease, fire, harassment, theft, aggression, and attack from internal and external forces. Acceptance or tolerance of violence and other causes of harm in schools often parallels tolerance of violence in the surrounding neighborhood and community, as well as norms within the state or nation. Violence in schools that parallels violence in the community includes theft, corporal punishment, sexual assault, rape, gang attack, hate crimes, and murder.

The worldwide concern for school safety has not evolved into a common commitment to the use of security-related technology or development of standards to guide that use. Application of such technologies is inconsistent due, in part, to the differences in and fragmentation of systems, often in the same state or nation. In most nations, there is no central authority that dictates type or use of safety and security technology or assesses its impact on preventing and intervening in violence.

Generally, the better-funded schools in developed and some developing nations tend to use some or all of the most common types of school security technology. These include computer and social media alerts, identification card or biological access control, panic and alarm buttons, scans of social media, use of mass messaging software for prevention and response, video surveillance, and visitor management (Reference 387).

The most basic forms of school security technology—the use of door locks, lighting, and alarms—are not universal. In developing and underdeveloped nations, as well as some developed countries, the struggle to obtain the basic essentials for learning such as teachers, teacher aides, student healthcare, books, paper, computers, and room lighting take precedence over security-related technology. Fire alarms and fire suppression technology also take precedence over security technology in schools.

Action to prevent violence in schools often is left to individual classroom teachers rather than a centralized officer or school administrator. In some nations, schools are not part of a system; instead individual villages, tribes, ministries, parishes, and other small community-centered organizations run them.

In 2010, the World Health Organization (WHO) outlined four broad steps for nations to consider in preventing violence in schools:

- **Surveillance:** Gather and analyze data to understand the extent and nature of the problem.
- **Risk factor identification:** Identify risk factors associated with injury and violence.
- **Intervention development:** Develop intervention strategies and tactics to address causes and evaluate the strategies and tactics when put into place.
- **Implementation:** Enable effective programs focusing on prevention.

Although most of these suggested steps involve policy, education, and behavioral change, technology is needed for data collection, information sharing, and other preventive measures. WHO noted that research is needed on the effectiveness of school violence prevention strategies in use worldwide (Reference 173).

Religious organizations (e.g., parochial schools, missionary schools) operate schools throughout the world. There are few references in the literature on the influence of religion and ethnicity on school violence in these facilities (Reference 376). Most of the literature on religion and ethnicity as a cause of

or contributor to violence in schools makes reference to government-regulated schools. Parochial schools vary as much as public schools in structure and in many nations are unregulated. Ultra-orthodox religious schools tend to address school violence differently than do other parochial schools. Administrators in some ultra-orthodox schools refuse to address school violence, verbally or through policy and tactics, over concern that recognition and discussion might implant ideas about wrongful behavior (Reference 323).

14.2 POINTS OF FOCUS

There is no global clearinghouse or database that provides collective information on school safety.

Accurate international data on type, quantity, application, and assessment of school security technology designed to prevent violence are slight. The difficulty in studying school safety and security internationally was cited in a 2007 Eastern European study conducted by UNICEF and the Commonwealth of Independent States. The study report (Reference 288) asserted that global data on school safety is lacking and that information-gathering in many nations is dependent on the institutional memory of teachers and principals. The report noted that benchmarks on school safety and resulting data on implementation of systems and technology are limited. In many nations, simple benchmarks to measure safety in schools do not exist.

Schools in much of the world are part of a fragmented system or no system at all.

Decisions including those related to security and the purchase and use of technology are made independently of a central authority and often without national, state, or regional guidelines. In many locales around the world, community leaders (political, military, and tribal) dictate decisions for schools regarding technology and other resources without input from educators or security experts.

Schools in less-developed areas focus on preventing different events than schools in developed areas.

Schools and school systems in developed nations focus heavily on preventing and intervening in catastrophic events such as active shooters. In recent years, developed nations have sought technological approaches to preventing and intervening in bullying and other forms of aggression (Reference 159). In less-developed and poor nations, schools tend to focus on preventing culturally tolerated violence such as gender-based assault within the school and theft and aggression committed by people in the immediate neighborhood or region (Reference 37).

A common concern is a pattern and high incidence of violence against immigrant students.

Immigrant students are differentially affected regardless of the characteristics of the school (e.g., grade level, size, resources, and location) (Reference 293). Immigrant students are less likely to have access to support—response by and trust in the police, access to teachers and counselors, and transportation—to assist in preventing and responding to acts of violence. In addition, immigrant students, including refugees, bring their experiences and attitudes toward school violence with them when they enter a new school. This includes experience with technology to support school safety such as the use of social media (Reference 211).

In schools worldwide, including those in some developed nations, violence committed by teachers and school officials is tolerated.

Sexual assault and use of corporal punishment by teachers and other school officials is tolerated informally and by policy in some countries around the world. In a few nations, extreme aggression against students and student aggression against teachers is tolerated (Reference 95).

In many nations, there are limited fiscal resources and infrastructure to support basic or advanced school security technology.

Schools in developed and undeveloped countries may not have the infrastructure for school security technology. They often lack electricity, lighting, and doors and they struggle to obtain books, clean water, and other basic necessities.

14.3 BACKGROUND

Violence in schools and the harm it causes young people and others is not unique to the United States. School violence and, in particular, mass casualty events in schools worldwide continue to garner headlines and drive people's concerns and fears. In the September 2004 siege of a school in Russia, more than 350 people including more than 150 children were killed. In March 2009, a 17-year-old student killed 15 people at Albertville Technical High School in southwestern Germany. In April 2011, a gunman killed 12 children and wounded many others at a public elementary school in Rio de Janeiro. In 2008, 10 people were killed in a school in Finland. The incident replicated an incident only 1 year earlier in which 11 people were killed. Although studies of school violence focus extensively on developed countries, incidents in which students, teachers, and others are harmed in and near school are not limited to industrialized societies (Reference 28).

Ensuring a safe learning environment for students is a major responsibility of educators and policy-makers around the world (Reference 5). Cultural norms tend to dictate all aspects of school safety including use of school security technology.

Another international study of school violence was jointly undertaken by the University of Southern California and Hebrew University. It examined data comparing U.S. and Israeli schools. The study confirmed that school violence is a global problem and that lower grade levels (i.e., elementary) were most vulnerable. Fear of victimization was found to be the primary cause for people bringing a weapon to school, surpassing revenge, jealousy, or other causes. The study suggested a "whole-school approach" to school violence in which school leaders, students, parents, and other stakeholders play a role in identifying specific problems and means to resolve them, including the application of technology (Reference 197).

Studies show that violence in schools in some developed nations, such as France and England, is most common in institutions that serve primarily disadvantaged and marginalized students (Reference 263). Worldwide, the poorest schools are most vulnerable to repeated acts of violence, but are less likely to have access to advanced prevention and response technology.

Many of the global efforts toward securing schools, including use of technology, stem from study of and reaction to past events. Most common is the emphasis on mass casualty events and attacks by people external to the school. Focusing primarily on the type of mass casualty events that have occurred in the past results in limited thinking about prevention and preparedness for a broader range of risks to schools (Reference 92), such as suicide, strong-armed robbery, one-on-one and group assault on

students and teachers, gang intrusion, kidnapping (e.g., family-connected, human trafficking, and financial gain), and rape and sexual abuse.

14.4 CHALLENGES IN DEVELOPING AND UNDERDEVELOPED NATIONS

In the United States and other developed nations, school security technology is becoming commonplace. For example, schools in Austria, Spain, the United Kingdom, and other European nations use security personnel, weapons detection devices, authorized entry controls, video surveillance, and other security solutions. Many European nations have adopted a “whole school approach,” which involves technology, student and community education, policies and procedures, support for teachers, and more (Reference 323).

However, in developing and underdeveloped nations—and some of the poorest schools in developed nations—school security technology is limited or nonexistent. Applying a “developed nation standard” of school safety and security to schools worldwide is ineffective. The school-related issues, along with an overwhelming array of societal issues experienced in developing and underdeveloped nations, are vast and complex. Based on findings across the literature, the following is a brief sample of the issues that compound discussion of school security and application of related technology internationally:

- Funding for education is a secondary or low priority.
- School facilities are limited, often lacking space, power, heat, sanitation, and water.
- The crime culture of schools—including tolerance of large-scale sexual abuse, assault, and robbery—parallels occurrences and tolerance in the surrounding community and in society.
- Class, race, religion, sex, and other forms of discrimination are tolerated in schools.
- Communication between individual schools and oversight systems and government agencies is weak.
- Corporal punishment by teachers—at times, severe—is accepted within the school culture.
- An inordinately high number of students belong to gangs or similar groups.
- Access to police protection and response to crisis situations by government authorities is inadequate or nonexistent.

Schools in all parts of the world (including South America, Africa, Asia, and the Middle East) often are makeshift facilities and lack basic lighting, door locks, lavatories, privacy for boys and girls, and other essentials. Security technology is nonexistent or limited to securing school supplies.

14.5 PERSPECTIVE ON SCHOOL SECURITY TECHNOLOGY, WORLDWIDE APPROACHES, AND GLOBAL CONFLICT

Violence continues to occur at a high rate in schools in developing and underdeveloped nations, as well as industrialized countries, and has had an adverse effect on learning and, ultimately, community and economic development. Research shows that the widely held perspective that school violence is primarily an issue of industrialized countries has little basis in fact. It further shows that media portrayal of school violence as occurring primarily in industrialized nations is misleading (Reference 262).

In many parts of the world, governments that should be supporting safe schools in fact tolerate and, in some locales, are among the perpetrators of school violence (Reference 28). Schools, students, and teachers in some developing nations and in countries experiencing internal conflict and war are targeted and victimized routinely (References 125 and 181).

It is difficult to generalize about use of school security technology by nation. As in the United States, schools in some communities are well-equipped with technology and well-prepared to prevent and

respond to violence, while other schools a short distance away may lack basic security technology. In some nations, government forces, insurgents, tribes, terrorist organizations, and other groups destroy or steal the existing structure (e.g., power, communications) needed to make the technology work.

14.5.1 OVERVIEW OF SCHOOL VIOLENCE AND TECHNOLOGY IN A SELECTION OF NATIONS

This subsection provides an overview of the violence occurring in schools worldwide. It provides a cross section of nations and a perspective on school violence and the extent of the issues that could influence or be influenced by security technology. Included are some nations embroiled in internal conflict, war, rebellion, large-scale drug crime, and terrorism. Some of the information was collected by the Global Coalition to Protect Education from Attack and is based on a 2009–2013 study of 70 “conflict-affected” countries (Reference 289). Additional information was collected by the study team. Security technology is limited in most or all of the schools in these nations.

In 2015, the United Nations Office for Disaster Risk Reduction sponsored an international conference as part of its Worldwide Initiative for Safe Schools. An outcome of the conference was a pledge by 24 nations to ensure the basic right of students to attend safe schools. The conference focused on safety related to natural disasters (e.g., earthquake, storms, floods) as well as other causes of harm. Emphasis was placed on the importance of technology, although there was no specific mandate; rather, there was an agreement to explore and share promising practices. The participating nations included Armenia, Cambodia, Costa Rica, Ecuador, Georgia, Islamic Republic of Iran, Italy, Japan, Kazakhstan, Kyrgyzstan, Lao PDR, Madagascar, Mexico, Nepal, Nigeria, Panama, Qatar, St. Vincent and the Grenadines, South Africa, Thailand, Tunisia, Turkmenistan, Turkey, and the United States (Reference 217).

The nations cited in the following subsections represent a cross-section of regions, size, economic status, and experience with and response to school violence. They were selected based on availability of information. Limitations of staffing and budget precluded review of a larger number of nations.

14.5.1.1 Afghanistan

In recent years, Afghanistan has been one of the nations most adversely affected by violence in schools. Violence prevented approximately 5 million students from attending school in 2010. In Afghanistan, 439 teachers, school employees, and students were killed between 2006 and 2009, one of the highest rates in the world (Reference 98).

The United Nations reported more than 1000 attacks on schools between 2009 and 2012. This included schools being set on fire, suicide bombings, and remotely detonated bombs set off in schools. Threats against school staff and abduction of teachers and students occurred with increased frequency. The actual number of incidents is unknown.

Support for technology is minimal. Approximately 40% of students attend classes in buildings; the other 60% have no school facilities. Throughout Afghanistan, many students attend “desert schools,” which are gatherings of students and teachers in areas outside of villages and towns. In an effort to modernize the educational system, 4500 new schools are planned (Reference 98).

14.5.1.2 Australia

In one 12-month period in the State of Queensland, more than 50,000 students were suspended—one-third of them for acts of physical violence. In South Australia, teachers reported 3000 violence-related injuries. Rural schools in Australia reported a higher rate of violence than metropolitan and urban

schools (Reference 59). These and other incidents led to Australia undertaking a significant national focus on preventing school violence. The National Safe Schools Framework provides Australian schools with guiding principles that assist schools and communities in developing practical student safety and wellbeing policies and practices. The Australian government collaborates with state and territory governments to support the Framework, which references responsible use of technology, monitoring misuse of technology, and focusing on emerging technology related to student safety and well-being. It specifically cites use of prevention-related technology in the classroom and on playgrounds (Reference 327).

14.5.1.3 Bahrain

Following the outbreak of anti-government protests in 2011, students, teachers, and academics were arrested and removed from schools. Teacher association leaders (i.e., labor leaders) were imprisoned. Sectarian threats and intimidation in schools and universities remain commonplace. An effort to reform schools and curricula in Bahrain includes priority focus on school safety and security. Students who have access to social media rely on it for communication and routinely share information about safety and security (Reference 80).

14.5.1.4 Central African Republic

The Central African Republic serves 788,000 students in primary and secondary education. Most of the nation's students are young, with more than 80% (662,000) enrolled in primary education. According to the United Nations, the school system in the Central African Republic is "on its knees" because of the ongoing civil conflict (Reference 99).

The four levels of education—nursery, primary, secondary, and tertiary—have been devastated by a civil war that has lasted for decades (Reference 122). Most attacks on schools took place after the Séléka rebellion in late 2012 and during 2013. More than 100 schools were damaged, destroyed, or looted. Two dozen schools were commandeered for use as military bases. There were reports of students and teachers being killed in the takeovers, but this has not been substantiated. By early 2013, one in two schools had closed. According to UNICEF, approximately 70% of primary school students have not returned to school since the conflict began in 2012 (Reference 350).

International organizations are working to reinvigorate the schools, but progress has been slow. By the end of 2013, 20,000 schools had received school supplies. Some schools received furniture and basic essentials to re-open. Security technology is minimal.

14.5.1.5 Colombia

A law in Colombia requires at least 10% of the nation's budget be allocated to education (Reference 105). All students in Colombia wear uniforms to minimize violence, bullying, and other clashes based on economic and other differences. The school system relies heavily on private schools; for example, more than 40% of the secondary schools are private (Reference 105). Generally, security in private schools exceeds that in government-run schools and includes full-time security personnel, electronic monitoring, gates and fencing, and other measures. Although educational achievement and literacy in Colombia are high, there is disparity between urban and rural areas.

From 2009 to 2012, approximately 150 school teachers were murdered and more than 1000 received death threats. Threats against school teachers increased in 2013 (Reference 130).

Armed groups routinely enter schools to recruit children and to sexually assault students. Reports of public security forces using schools for military purposes continue despite legal prohibitions. An increased number of parents send their children to residential schools, which they believe to be safer than others (Reference 69). Prevention is based primarily on awareness and personal protection rather than technology.

14.5.1.6 Côte d'Ivoire

Across the country, only half of the students between the ages of 6 and 11 attend school; in rural areas, the percentage is even smaller. Almost one-third of secondary schools are parochial. The nation suffers from a lack of teachers and either no or poor school buildings. Access to any form of technology is limited. During the 2010–2011 post-election crisis, armed groups and military forces destroyed, damaged, and looted approximately 500 schools and universities. Schools were routinely commandeered by these groups for use as bases of operation (Reference 131).

14.5.1.7 Democratic Republic of the Congo

Despite expending approximately 6% to 7% of the national budget on education and providing free primary education (based on a 2010 law), more than 7 million children do not attend school (Reference 3). This includes 60% of the nation's adolescents. Generally, school infrastructure and resources cannot support security technology. Many schools lack desks and chairs (students sit on floors), blackboards, and other core essentials. The illegal acquisition of school land by businesses and others inhibits progress (Reference 160).

Attacks on schools, including widespread looting, damage, and destruction of facilities, are more commonplace today than in past years. Armed groups routinely recruit school students. Students and teachers fear being abducted. In the eastern provinces, attacks on schools have forced them to shut down and cease teaching.

14.5.1.8 Egypt

In Egypt, approximately 7.9 million students attend 40,900 schools (Reference 21). Primary and secondary education is mandatory, and 95.4% of the eligible population is enrolled in school. According to UNICEF, although 92% of the students attend government-run schools, access to public system infrastructure, trained teachers, and other resources (including technology) is limited (Reference 104). Like other nations in which security technology is limited, schools in Egypt rely on awareness, training, and personal safety as a means to reduce violence.

A study conducted by the National Center for Sociological and Criminological Research stated that children are among the most vulnerable groups in Egypt when it comes to exposure to violence. To address the growing concern over assaults against youth, the Egyptian government established a National Plan for the Elimination of Violence Against Children in 2006; however, the effectiveness of the initiative has been questioned (Reference 337).

According to a 2010 study, 119 students died as a result of violence, 206 were sexually harassed or assaulted by teachers or school employees, 336 were injured by teachers, and 253 were injured as a result of unsafe school facilities (Reference 199). The Secretary General of the National Council for Childhood and Motherhood reported that a 2014 study revealed that attacks on children increased by 55% between January and October compared with the previous 3 years. Fifty percent of the incidents

occurred in schools. Some experts believe that escalating violence in Egyptian schools is a result of the unstable conditions that have permeated the country over the past 4 years (Reference 199).

Although a recent initiative allowed schools to apply for government funds to improve infrastructure, school facilities throughout Egypt are in poor condition. This poor condition and lack of funds has prevented large-scale implementation of security technology. Many schools lack the basics—alarms, entry security, and lighting.

Political and sectarian tensions led to sporadic attacks against lower grade and secondary schools and damage to and looting of schools and universities. Students and teachers were injured. Both government and non-government forces were blamed for the attacks and the resulting damage to school facilities.

14.5.1.9 Ethiopia

Currently, Ethiopia is among the 20 poorest nations in the world, according to 2013 World Bank and International Monetary Fund data. UNICEF reports the age of more than half the nation's population is younger than 18 years. A primary concern in Ethiopia is widespread tolerance of sexual violence in schools. Numerous studies report an extraordinarily high percentage (some as high as 75%) of young girls in schools being sexually assaulted (Reference 200). Arbitrary arrest, ill treatment, and torture of students were documented and particularly affected those of Oromo ethnicity. Older and university students also were targeted.

14.5.1.10 Germany

Since 1999, Germany has experienced more than a dozen serious incidents of targeted school violence resulting in multiple casualties. In a 2009 incident near Stuttgart, a student killed 15 people and injured 14 others before killing himself. Other incidents followed in schools in Bavaria, Erfurt, Emsdetten, and Winnenden. These incidents prompted a national effort to advance prevention that included expanding the number of counselors, expanding programs to prevent bullying, and implementing seminars for teachers and parents. The incidents also led to political pressure to advance school security technology.

The Committee on Internal Affairs of the German Parliament addressed whether students should be screened for weapons when entering schools. Specifically, members of Parliament discussed the use of metal detectors and radio frequency identification chip card systems. After much debate, Parliament declined to implement the use of these technologies on a nationwide scale.

Other technologies have been implemented across schools in Germany. A national Security in Schools initiative provides support to schools seeking technological approaches to preventing and responding to violence. Alarms, special locking systems on classroom doors, color-coding facilities to guide first responders, and pagers and cell phones for school staff are commonplace. Video cameras are less common, with implementation slowed due to budget constraints. Use of security officers in schools is uncommon in Germany; only a few districts, such as the Berlin district of Neukoln, deploy them. Where security officers are employed, they are minimally armed, often carrying only cell phones.

To fill the gap between traditional prevention practices and those needed to address major incidents such as active shooters, German authorities began the Berlin Leaking Project. This effort examined the viability of preventive efforts based on early identification of "leaking behavior." Leaking refers to any behavior or communication that indicates one or more students are planning to carry out a violent attack. Leaking behavior often precedes acts of school violence (Reference 203). The initiative involves

engaging teachers and others in identifying explicit and implied threats of violence, fascination with prior acts of violence, and evidence of planning or preparation to carry out an attack. Identifying such behavior includes focusing on verbal cues and behavioral changes, rumors and school gossip, and monitoring social media. Once identified, a school-based team evaluates the student and initiates interventions, which may include mental health services and the involvement of law enforcement agencies (Reference 203).

All schools in Germany have been charged to develop emergency management plans; approximately 70% of schools have done so. A 2011 survey of 1800 schools showed that 170 had implemented their plans, which often included use of alarms and technology to enable response to shooting-related threats (Reference 88).

14.5.1.11 India

School violence in India costs the nation \$7.42 billion annually, which in dollars and social impact exceeds the combined cost impact in Bolivia, Colombia, the Dominican Republic, Ecuador, Egypt, El Salvador, Guatemala, Jordan, Nicaragua, and Peru combined (Reference 271). Although corporal punishment in schools has been made illegal, teachers continue to use it widely. In one survey, 65% of students reported being beaten by their teachers (Reference 332).

According to one study covering 2009 to 2012, militants attacked approximately 140 schools (Reference 133). There was widespread use of schools as barracks or bases by government forces, mostly in the eastern part of the country. Kidnapping of students in school and while on school buses is prevalent. Use of global positioning system tracking devices on school-owned buses and text messaging with parents are being employed to minimize risk of kidnapping, but many students rely on private transportation or walk to school (Reference 352).

A study on social adjustment of eight and ninth graders in India showed that violence in homes and communities impacts the achievement of students and their attitude toward violence in school. Male students tend to be victims of beatings and psychological violence in their homes, whereas female students tend to be victims of sexual assault (Reference 84). Approximately 70% of students who said they had been assaulted did not report the incident, claiming the violence is condoned or would be ignored (Reference 315).

School security is improving throughout India, but change is occurring slowly (Reference 352). Increased emphasis is being placed on the use of security officers at gates and other entrances. Communities with stronger fiscal support and wealthier private schools are employing technology including surveillance cameras. Use of social media for prevention and communication in a crisis is increasing.

14.5.1.12 Israel

Violence is prevalent in Israeli schools, but less so than in many other nations. Fighting, bullying, sexual harassment, and verbal abuse have been cited in various studies as concerns. From 2010 to 2012, school violence in Israel declined by 25%, according to a study by the Israeli Health Ministry. The decline is attributed to advances in prevention and increased support for teachers and school administrators in dealing with actual and potential student problems (Reference 251).

In 2015, the Education Ministry introduced new guidelines to address school violence, recognizing that technology such as social media can be used to promote and exacerbate violence (Reference 138). The new guidelines also recognize that technology is used to drive issues in the community and in the

school. The guidelines state that personal technology can only be used in school for educational purposes. They also allow school use of social media to communicate with parents and others.

Schools throughout Israel employ security technology extensively. The technology ranges from basic, such as perimeter fencing, to advanced, such as use of metal detectors. Schools also employ armed private security officers. Some schools also rely on armed teachers and armed teacher response teams (most involved have military experience). Although Israel allows teachers to be armed, only a small percentage carries guns (Reference 78).

The relationship between the police, the Israeli Defense Forces, private security firms, and schools is closer than in most other nations. Private security officers in schools must undergo weapons and general security training and pass physical, criminal, and mental health screening (Reference 167).

Among the advances, starting in 2014 schools throughout Israel were provided with a location-based detection system that monitors the location of security personnel. School security and police officials know where their security personnel are in real time and are able to direct primary and secondary response, coordinate student and personnel safety, and improve overall efficiency when dealing with a crisis (Reference 311).

14.5.1.13 Kenya

There is a long history of school violence in Kenya. In sporadic attacks on schools, students and teachers have been murdered by militants or troops. Tribal attacks on schools also occur. Students are targeted and have been killed while traveling to and from school.

Focus on reducing violent behavior is gaining expanded attention. Crimes in schools across Kenya include attacks on individuals, ethnic violence, and full-scale rioting by students in secondary schools. It also includes large-scale sexual assault of students, referred to in one study as “mass sexual assault.” One study reported that 58% of students are sexually assaulted while in school (Reference 294). In a study of 6,354 teachers and 65,969 students, priority needs to reduce school violence included laws against sexual assault, rigid enforcement of the laws against sexual assault, bans on the caning of students, and implementation of prevention tools including use of technology where capability exists (Reference 277).

In response to increasing acts of school violence and inconsistencies in the ways in which schools respond to them, the Kenya Ministry of Education produced and distributed a Safety Standards Manual. The goal of the manual is to establish a more consistent approach to violence prevention and crisis management across schools. The manual cites application of varied resources, including technology. Despite the national effort to effect change and the publication of national standards, lack of funds and inadequate supervision have inhibited progress. Use of technology is curbed, in great part, by lack of and poor infrastructure (Reference 391).

14.5.1.14 Mali

There are approximately 8700 primary and secondary schools in Mali, staffed by approximately 36,000 teachers. The primary and secondary school student population exceeds 1.6 million (Reference 252).

There is significant disparity in education and educational facilities between urban and rural schools. Weak infrastructure constrains the implementation of security measures in many schools.

According to the United Nations Children’s Fund, violence in Mali’s northern region over the past 4 years has forced hundreds of schools to close, caused thousands of students to stop attending school, and caused 600 teachers to resign. Violence in the region prevents approximately 400,000 students from attending school. In one area of Mali, 280 schools closed and have remained closed for 3 or more years. In another area, 130 schools were looted, destroyed, or used by armed groups and government forces during fighting (Reference 363).

According to the United Nations Office for the Coordination of Humanitarian Affairs, some schools have reopened in the areas of conflict. However, teachers failed to return and therefore volunteers are providing instruction. In the areas in which facilities have reopened, less than half of the students have returned due, in part, to fear associated with continued conflict and lack of security measures in the schools (Reference 143).

14.5.1.15 Mexico

For more than 15 years, enrollment in Mexican schools increased dramatically. Approximately 200,000 schools in Mexico serve more than 25 million students and employ 1.6 million teachers (Reference 66).

Violence in schools has been identified as a crisis and, according to UNICEF, is one of the main reasons students drop out before graduation and miss school for extended periods. Threats against teachers and bomb threats in schools and universities increased significantly since 2010. From 2009 to 2012, more than 50 students, teachers, and education officials were killed or abducted, with their whereabouts unknown (Reference 134).

In Acapulco, 22 teachers were killed and 8 were kidnapped from schools. The crimes were attributed to organized crime. This promoted the assignment of police to 80 schools and a major effort toward prevention. New security measures, including improved entry and monitoring systems and the presence of full-time or part-time security personnel, were implemented in 110 schools (Reference 134).

Reforms in Mexico place priority on improving school attendance (Reference 81). Among the reasons students fail to attend are fear, threats, injuries, and fluctuations in the economy that drive parents to take students out of school to go to work.

Activities resulting from a mandate of the 2013 Constitutional Reform of Education initiative are underway to implement a modern nationwide information system to support education. This effort includes a wide range of activities including state-of-the-art technology, software development, enterprise architecture design, and data management. Advancing the initiative requires attention to the vast array of educational cultures, environments, fiscal constraints, and willingness of communities to engage. It includes a focus on school safety (Reference 366).

Also in 2013, Mexico established a new Commission for the Prevention of Violence and Criminality. The Commission receives \$9.2 billion to help discourage young people from joining criminal organizations. One of the priorities of the Commission is to lower school violence. Policies, including extending school hours, are being implemented. It is anticipated that infrastructure improvements, including use of security technology, will be supported in as many as 40,000 schools.

14.5.1.16 Russia

Russia has approximately 60,000 schools. In 2014, the Pearson/Economist Intelligence Unit rated Russian education as the 8th best in Europe and 13th best in the world. Russia has the highest rate of college attendance (per capita) of any nation in the world (Reference 268).

In 2004, a school siege in Beslan in North Ossetia resulted in one of the most deadly assaults on a school in history. The 3-day siege, led by insurgents, resulted in the death of 385 people including 186 children. The attack brought worldwide attention to the vulnerability of schools to terrorist attack.

More recently, following a series of bombings against residential apartment buildings in Moscow, an effort was undertaken to improve security in schools. Use of security technology such as closed-circuit television (CCTV) and surveillance cameras increased. Further security measures, including the hiring of security guards, were contingent on funding from parents (Reference 266).

In 2014, a hostage taking and Russia's first in-school shooting resulted in the death of a security officer and teacher, and prompted major reform in school security. CCTV and panic buttons were installed in all Moscow schools. Turnstiles and other electronic entry systems were installed at the entrances of some schools. Schools deemed to be at higher risk because of the surrounding community and other variables received steel fences and walls. Moscow officials continue to debate the value of metal detectors (Reference 260). Many of the reforms are being funded by the local government.

Locales in other parts of Russia have not advanced school security to the same degree as is occurring in Moscow. Among the reasons for this lower priority are a lack of serious and headline-grabbing incidents, fiscal issues, and infrastructure problems.

14.5.1.17 Turkey

More than 16 million students attend 65,000 schools in Turkey. Fear of harm and exposure to political violence and drugs inhibit student attendance and general progress in education. In the areas of Turkey that border Syria, violence from the Syrian civil war has harmed Turkish communities (Reference 79).

Between 2010 and 2012, two dozen schools were bombed or set on fire primarily as a result of political strife. During the same period, 28 teachers were abducted. Incidents occur primarily in the south, east, and southeast where Kurdish insurgents are active (Reference 135).

In January 2016, five students were injured in a school in majority-Kurdish southeast Turkey when a hand grenade was thrown into the schoolyard. In the same month, a rocket launched from Syria hit a school, killing a school employee and injuring a student. Two other rockets hit the field adjoining the school (Reference 166).

Technology to reduce threat is limited to entry security and CCTV. Security technology is less visible in rural area schools. Primary emphasis has been placed on the use of the Turkish National Police to provide concentrated patrols around schools. In addition to preventing political clashes from interfering with schools, the patrols are focused on preventing drug sales to students and other drug-related crimes (Reference 144). In 2014, a decision was made to assign a police officer to almost every school (Reference 79).

14.5.2 STUDY OF SCHOOL-BASED VIOLENCE IN FIVE ASIAN NATIONS

In 2014, a study of five countries in Asia—Cambodia, Indonesia, Nepal, Pakistan, and Vietnam—was conducted by a collaboration of several organizations. The primary purpose of the study was to assess the prevalence of gender-based school violence, response to the violence, and the reporting of violence. The study involved interviews with 9000 students from the five nations about their experience with school violence (Reference 275).

The research found that much of the violence in schools in these five nations is based on inequitable gender attitudes. The frequency and seriousness of the violence has created a culture of fear and a lack of safety in schools. Implementing prevention tactics, including use of technology, is inhibited, in part, because gender violence is accepted in the culture. Teaching and non-teaching school staff perpetuate gender-based violence. As a form of discipline, teachers and staff also engage in non-gender-based violence (e.g., general corporal punishment) toward students. Intervention and reporting by students, staff, parents, and others is low due to fear of repercussion and lack of “coherent response mechanisms.” The study suggests that violence in schools in the five nations has become “normalized” (Reference 275).

The study notes that violence in schools is compounded by lack of specific laws and lack of enforcement of existing laws. Technology-based tools to reduce violence in these countries, such as use of social media, alarms, and monitors, are used minimally.

14.6 CONCLUSION

School safety is a global concern. This review of school security internationally was undertaken to complement the study of school security technology in the United States, particularly as it relates to preventing and responding to acts of violence.

According to WHO, UNICEF, Amnesty International, and other organizations, preventing violence in schools is a priority among many nations. However, although preventing school violence is a common goal, there is little consistency in use of school security technology across nations, states, regions, and communities. There is tremendous disparity in the attention given to school safety among developed, developing, and underdeveloped countries (status based on per capita income, literacy rate, living standard, etc.). Differences exist in causes of violence, resources, laws, policies, procedures, access to technology, infrastructure, measures of effectiveness, and desire to effect change.

Literature on school violence internationally was reviewed. National data on use of security and safety technology in schools do not exist in the vast majority of countries. Academic publications, popular media, and international organization reports tend to address causes, needs, and proposed and actual solutions. References to security technology in the literature (both academic and popular) are minimal, particularly in addressing school violence. Data on expenditures and outcomes directly related to school security technology are also slight, with reports on the value of the technology based on small studies that are difficult to generalize or on anecdotal information (Reference 83).

Schools and school systems worldwide focus on preventing violence caused by hate, extremism, religion, drugs, and gender inequity. They also focus on violence generated by intrusion into schools by gangs, extremists, revolutionaries, militia, military, and other groups. Kidnapping, murder based on politics or ideology, rape and sexual assault, and beatings are frequent occurrences in schools throughout Africa, South America, and the Middle East.

It is difficult to compare school security in the United States to other nations. Although U.S. schools are safe places, school-based shootings have occurred more frequently in the United States than in other countries (Reference 261). Countries such as Germany, Finland, Russia, and Israel also have experienced mass shootings and other types of mass casualty incidents in schools and have given attention to preventing future attacks.

Funding of security technology around the world is uneven and often competes for other priorities such as basic educational supplies. One study estimates that spending on surveillance and access control systems in schools in all of the Americas is approximately \$300 million; of that total, \$210 million is spent in the United States alone (Reference 229).

Schools in developing and underdeveloped nations and in rural and tribal areas of developed nations may lack the infrastructure for advanced school security technology. They often lack electricity, lighting, and doors and they struggle to obtain books, clean water, and other basic necessities. For example, the “desert schools” in several nations hold classes in open areas away from towns and villages. In Mexico, some government and private schools have advanced security technology and security personnel, but a short distance away other schools have inconsistent or no electric power.

Violence and fear of harm caused by violence in and near schools will continue to be a focus of attention in the United States and other nations for the foreseeable future. For example, annual global expenditures on surveillance and access control systems in schools (independent of other technologies and security measures) is expected to grow by approximately 14% annually and will exceed \$1.1 billion by 2018 (Reference 229). Access to and deployment of this technology, however, will be highly variable in nations around the world.

This page intentionally left blank.

Chapter 15. CONCLUSION

William R. McDaniel, PhD, and Steven R. Taylor, MPA

Incidents of extreme violence at schools both in the United States and abroad have resulted in increasing public and political scrutiny and a call to assess ways to secure U.S. classrooms and campuses more effectively. A broad range of technologies can be applied to improving school security and safety, including low-technology devices such as lights, doors, locks, and door pins, and at the other end of the spectrum metal detectors, “smart” surveillance cameras, social media analysis tools, infrared detection, and sophisticated school-to-police communication systems. These technologies are being used in varying degrees in schools throughout the United States.

This comprehensive review of school safety and security technologies reveals much about the current state of practice of such technologies across U.S. schools. The specific objectives of this report are to:

- Identify technologies currently being used in K-12 schools to prevent, respond, and mitigate criminal acts of violence.
- Identify how the technologies are being used (i.e., purpose, policy, and practice).
- Identify what is known about the efficacy of those technologies.
- Identify factors such as laws, policies, regulations, and costs that affect deployment and employment of technologies.
- Provide reports and other information to the National Institute of Justice (NIJ) for dissemination to the various constituents that play a role in safety and security in schools. (Reference 360)

The study team approached these objectives using four different research components—a literature review, a technology review, case studies, and a legal review. These complementary components, separately offering the views of academics, engineers, practitioners, and policy makers, demonstrate the competing demands and constraints placed on schools and law enforcement as they keep schools safe. Together, they reveal the how and why of different approaches to school safety.

Objective 1: Identify technologies currently being used in K-12 schools to prevent, respond, and mitigate criminal acts of violence.

To reach the first objective, the study team categorized technologies by their technical area. The following areas were reviewed:

- Access control
- Alarms and sensors
- Communications
- Lighting
- Software applications
- Surveillance
- Weapons detection
- Other

The specifics on these areas are covered elsewhere in the report, but certain overall themes have emerged. For instance, these technologies may be sorted by their specificity to the task of preventing and mitigating criminal acts of violence, or even particular crimes. Communications, locks, and lighting are very general technologies present in most, if not all, schools that may be leveraged to prevent

crimes, but they are rarely thought of as being specific to crime prevention. One benefit of this is that these technologies are ensured regular maintenance, training, and operational use. Other technologies, such as access control and surveillance, are often thought of as safety-related, but provide additional benefits to schools where they are used. The improved ability to track the presence of visitors and school personnel facilitates overall operations and helps school officials direct their attention to other priorities, whether they are specific to safety or related to other issues. Alarms, sensors, and weapons detection may be more closely related to prevention of violent crimes, but come with financial and environmental costs because these more tailored technologies require regular training and maintenance; some can even change the atmosphere of a school.

Emerging software and other technologies are just now making their way into the K-12 market, leaving their ultimate impact undetermined. This is related to another theme that emerged, concerning the role of the K-12 market in the uptake of safety technologies, particularly as seen by the safety and security technology industry. Even for well-established technologies, schools rarely were the early adopters. It is often the case that technologies are developed for other applications and then migrate to schools to serve a particular purpose. Weapons detection technologies have been used in many environments, such as airports and courthouses, for years. However, their use in schools has increased with the rise of concern about active shooter incidents. Some technologies that have been developed more specifically for the school environment, such as visitor control systems tied to sex offender registries, grew because of perceived need, and accompanying government mandate.¹ Without specific driving examples of such a need, these technologies may never get the market support to develop and thrive.

The bounds of this objective also revealed a theme of technology use in schools. By limiting the review to K-12 schools and criminal violence mitigation and prevention, the report reveals the relative leeway that schools have to employ such technologies. In their role, both legally and within American society, as caretakers of minors, schools can employ monitoring and detection technologies in a way that a private company might not be able.² This is especially important as emerging computer surveillance technologies become more prevalent in schools. The cyber realm does not have well-defined physical boundaries in the same way that school grounds do, but the need for securing students' wellbeing may give schools more freedom than other institutions to investigate cyber activities. The implications of this are still to be seen, but will be important for school officials to consider as technology advances.

Objective 2: Identify how the technologies are being used (e.g., purpose, policy, and practice).

To meet the second objective, the study team concentrated on interviewing school and safety officials at various levels to uncover both the intended and actual uses of technologies. In interviews with education and law enforcement leaders at the Federal, state, and district levels, the study team gathered a deep understanding of the intended role of school safety technologies, which is almost uniformly as support to the individuals responsible for school safety rather than as a separate driver of school safety. Law enforcement and school officials face a daunting task in ensuring the safety of the millions of students attending K-12 schools each day. Information about students, staff, the school environment, the community, and threats that might be posed by any of them is essential. Technologies that provide the most up-to-date information about the safety situation of schools tend to be more desirable based on how much of this burden they can take from these individuals (e.g., school administrator, school resource officer, school safety and security administrator).

¹ <http://www.poynter.org/2009/only-one-state-has-adopted-new-Federal-sex-offender-law/99709/>

² <http://www.cnn.com/2013/11/08/living/schools-of-thought-social-media-monitoring-students/>

Another key theme that emerged was the limited utility of technologies that cannot be integrated with each other. Federal officials advocated for technologies that could easily share information, especially between schools and first responders. School officials shared this view, and further expressed either satisfaction with technologies that work together or frustration with those that do not. In addition, while most school principals and other officials reported concern about day-to-day offenses (e.g., assault, bullying, theft), much of the focus of security technology has been on the prevention of and response to active shooters and mass casualty events. Focus on low-incidence, high-consequence events has been a priority since the Columbine High School shootings in 1999. According to school officials who provided input to this study, the continued focus on mass casualty events is driven by funding (Federal and state grants), school system mandate, media focus on such events, public sentiment and fear, and a genuine desire to foster effective prevention and response measures. The assumption made by many is that a focus on the prevention of and response to major events will positively impact the prevention of and response to day-to-day and less serious violent offenses.

Objective 3: Identify what is known about the efficacy of those technologies.

The third objective proved to be the most challenging to meet. As noted earlier, there are several factors that make it difficult to find reliable metrics on the efficacy of these technologies.

- There is no comprehensive source to locate data about technology deployment for school safety. The National Center for Education Statistics collects data on a limited number of security technologies, but its survey is broad and not comprehensive. There are few state databases on school security technology, but these are not aggregated.
- Schools are not required to report on the type of security technology in place, how it is funded, or how it is selected.
- Although anecdotal evidence is frequently cited, few schools and school systems monitor, assess, and report on the use and outcomes of security technology.
- Criminal acts of violence within schools are relatively rare events, which is fortunate for schools but makes the scientific and data-driven evaluation of the efficacy of specific technologies difficult to accurately assess.
- Much of the general information and research on the effectiveness of school security technology is vendor-driven.

One mitigating factor is the effort, through training and publications, of associations and organizations at the national and state levels to disseminate information on school safety technologies in cooperation with schools and independent of vendors. Many organizations (e.g., National Association of School Resource Officers, National Association of Secondary School Principals) provide literature and training that reviews school safety technologies from the point of view of law enforcement and school officials, but this information is more anecdotal than the results of an analytic study would be.^{3,4}

The information provided by these organizations on safety technologies is in the context of an issue rather than a solution. This integrated, contextualized view of school safety demonstrates that metrics of school safety are difficult to isolate to a specific technology. The organizations generally measure the overall environment of schools and relevant issues faced by individual schools. Multiple law enforcement officials pointed out the seemingly contradictory observation that usually a school district's safety metrics will appear to get worse after an intervention when the actual environment is improving. One

³ <https://nasro.org/>

⁴ <https://www.nassp.org/?SSO=true>

concern in assessing crime rates is that it is difficult to know whether changes reflect real rates in crime or changes in reporting behavior. If improved safety leads to higher trust in authorities, then a rise in reported incidents, which would appear to be a negative indicator, is actually a positive one.

Objective 4: Identify factors such as laws, policies, regulations, and costs that affect employment and deployment of technologies.

The fourth objective further demonstrates the need for an integrated view of school safety. The team conducted a legal review (law and regulation), a literature review, and an international review as part of the study, each of which revealed different aspects of school safety technology implementation. The legal review shows the disparate approaches to school safety taken by different states and jurisdictions through law and policy, and how these different approaches might drive different technology decisions. Much of the existing law encourages schools to plan for safety and sometimes authorizes the use of safety technology in general, but the law infrequently mandates the use of specific technologies.

The literature review reveals important information about the role of technology in school safety, and the ways in which budget and organizational decisions can change how technology is considered and implemented. One highlight from that review, which was echoed by many school and law enforcement officials, was that funding for school safety often comes as a grant in response to an incident, such as the shootings at Sandy Hook Elementary School in 2012. This money sometimes comes with stipulations on what types of technology can be purchased, which can be a major driver of technology selection. A hidden risk with this phenomenon is the acyclic nature of funding. Technologies have an expected life cycle, and as equipment ages and technology advances, equipment and software must be replaced. Grants in response to incidents, however, almost never account for this, leaving schools with aging systems and no means to refresh the technology.

Following the shooting incident at Columbine High School, school violence became a global issue. Violence and threat of violence has affected and continues to affect communities in almost every nation in the world. The literature on use of security technology and its outcomes, particularly in developing and underdeveloped nations, is slight. Much of the information available on school violence and school security technology is based on media reports, local and regional data collection, and anecdote. Generally, the better-funded schools in developed and some developing nations tend to use some or all of the most common types of school security technology. In developing and underdeveloped nations and in some developed countries, however, schools struggle for essentials to support instruction. Assets such as teachers, teacher aides, student healthcare, books, paper, computers, and room lighting take precedence over security-related technology.

Objective 5: Provide reports and other information to NIJ for dissemination to the various constituents that play a role safety and security in schools.

The final objective begins with this report, but certainly does not end there. It is widely acknowledged that any report on “current” technology is outdated by the time of its publication. It is the hope of the study team that this publication highlights the need for continuing, objective study of school safety technologies. In addition to reports of this nature, processes and methods for regular technology review, including evaluations of technology effectiveness, are needed. These should be supported by web-based, frequently updated information sources that are easily searchable and available to school safety officials who are considering technology implementations.

It is also the hope of the authors that the information in this report meaningfully meets the needs of school officials who endeavor to make the nation's schools safer places. To the credit of these officials, U.S. schools are, for the most part, among the safest areas in U.S. society. As safety technologies advance, many have wide applicability to the K-12 environment and can and will continue to make schools a safe haven.

This page intentionally left blank.

Appendix A. REFERENCES

1. Achutan, C., and Mueller, C. (September 2008) "Evaluation of Radiation Exposure to TSA Baggage Screeners." *Health Hazard Evaluation Report*. HETA #2003-0206-3067.
<http://www.cdc.gov/niosh/hhe/reports/pdfs/2003-0206-3067.pdf>.
2. Addington, L. A. (2009) Cops and Cameras: Public School Security as a Policy Response to Columbine." *American Behavioral Scientist*, **52**(10), 1426–1446.
3. African Economic Outlook (2012) Retrieved from
<http://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/Congo%20Democratic%20Republic%20Full%20PDF%20Country%20Note.pdf>.
4. Aggleton, D. (May 2011) "Shedding light on illumination." *Security Technology Executive*.
5. Akiba, M., LeTendre, G. K., Baker, D. P., and Goesling, B. (2002) "Student victimization: National and school system effects on school violence in 37 nations." *American Educational Research Journal*, **39**(4), 829–853.
6. Albright, Matthew (31 October 2014) "Bulletproof whiteboard shields placed in school." *Delaware Online*. Retrieved 3 December 2015 from
<http://www.delawareonline.com/story/news/education/2014/10/30/bulletproof-whiteboard-shields-placed-school/18185965/>.
7. Ale, B. (2009) *Risk: An Introduction: The Concepts of Risk, Danger, and Chance*. Routledge.
8. ALICE Training Institute. "What We Do – ALICE Components." Retrieved 3 December 2015 from
<http://www.alicetraining.com/what-we-do/alice-components/>.
9. Allen, G., and Derr, R. (2015) *Threat Assessment and Risk Analysis: An Applied Approach*. Butterworth-Heinemann.
10. Anderson, M. et al. (2001) "School-associated violent deaths in the United States, 1994–1999." *JAMA*, **286**(21), 2695–2702.
11. Andress, J. (2014) *The Basics of Information Security: Understanding the Fundamentals of INFOSEC in Theory and Practice*. Syngress.
12. Arizona Department of Education (July 2015) "Answers to General Safety and Lockdown Questions." Retrieved 21 October 2015 from <http://www.azed.gov/special-education/files/2015/07/t3.8-q-a-lockdown-for-sped-students.pdf>.
13. Ash, K. (January 2010) "Student ID Cards Sport New Digital Features." *Education Week*. **3**(2). 32–33. <http://www.edweek.org/dd/articles/2010/02/03/02id.h03.html>.
14. Ashoor, R. "Safety Screenings: Syracuse City School District High Schools Reflect on Metal Detector Use." *The Stand*. <http://www.mysouthsidestand.com/more-news/safety-screenings/>.
15. ASIS International (2009) *Facilities Physical Security Measures Guideline*.
<https://www.asisonline.org/Standards-Guidelines/Guidelines/Published/Pages/Facilities-Physical-Security-Measures-Guideline.aspx>

16. Astor, R. A., Meyer, H. A., Benbenishty, R., Marachi, R., and Rosemond, M. (2005) "School safety interventions: Best practices and programs." *Children & Schools*, **27**(1), 17–32.
17. Atlas, R. (2013) *21st century security and CPTED: Designing for critical infrastructure protection and crime prevention*. CRC Press.
18. Babin, S. M., Cristion, J. A., Erekson, J. S., Gaither, M. F., Murphy, P. K., and Rodriguez, P.A. (2014) *Video Analytics Market Survey*, NIJ RT&E Center Project 13-8, Version 1.0.
19. Bachman, R., Randolph, A., and Brown, B. L. (2011) "Predicting perceptions of fear at school and going to and from school for African American and White students: The effects of school security measures." *Youth & Society*, **43**(2), 705–726.
20. Bachus, G. (1994) "Violence Is No Stranger in Rural Schools." *School Administrator*, **51**(4), 18–22.
21. Badr, M. (2012) *School effects on educational attainment in Egypt* (No. 12/05). CREDIT Research Paper.
22. Bannister, A. (2015) *How to Choose a PSIM Solution to Fit your Needs*. IFSEC Global. Retrieved from <http://www.ifsecglobal.com/choose-psim-solution-fit-needs/>.
23. Barrett, P., Zhang, Y., Moffat, J., and Kobbacy, K. (January 2013) "A holistic, multi-level analysis identifying the impact of classroom design on pupils' learning." *Building and Environment*, **59**, 678–689. Retrieved 20 October 2015 from <http://www.sciencedirect.com/science/article/pii/S0360132312002582>.
24. Battcher, D. (8 June 2015) "Fixed Wings, Quadcopter, and More." *Claims Management*. Retrieved 17 November 2015 from <http://claims-management.theclm.org/home/article/Fixed-Wings-Quadcopters-and-More>.
25. Bauer-Wolf, J. (6 August 2015) "Hood College's new drone gets grounded – for now." *Frederick News-Post*. Retrieved on 3 September 2015 from http://www.fredericknewspost.com/news/education/schools/college/hood/hood-college-s-new-drone-gets-grounded-for-now/article_f063df43-5cac-5c75-9918-b887d09451cd.html.
26. Beard, B., and Brooks, D. J. (2009) "Consensual security risk assessment: Overcoming bias, conflicting interests and parochialism." *Proceedings of the 2nd Australian Security and Intelligence Conference*.
27. Beger, R. (2003) "The 'Worst of Both Worlds:' School security and the disappearing Fourth Amendment rights of students." *Criminal Justice Review*, **28**(2), 336–354.
28. Benbenishty, R., and Astor, R. (2006) "School violence in an international context." Retrieved from www.ijvs.org/files/Revue-07/04.-Benbenishty-ljvs-7.pdf.
29. Berube, H. (December 1994) "New notions of night light." *Security Management*.
30. Bill to Arm Virginia School Officers with Stun Guns Advances (17 February 2015). *Security Magazine*. Retrieved 24 September 2015 from <http://www.securitymagazine.com/articles/86102-bill-to-arm-virginia-school-officers-with-stun-guns-advances>.

31. Birkland, T. A., and Lawrence, R. G. (2009) "Media framing and policy change after Columbine." *American Behavioral Scientist*.
32. Blackwood, J. (2014) "Timing is Everything: Physical Security Information Management (PSIM)." *Tech Decisions*.
http://www.corporatetechdecisions.com/article/timing_is_everything_physical_security_information_management_psim.
33. Blad, E. (2014) "School-Violence Tip Lines Get a Second Look After Sandy Hook: Additional states, districts discuss creating the reporting systems." *Education Week*. Retrieved from <http://www.edweek.org/ew/articles/2014/02/05/20tiplines.h33.html>.
34. Blitzer, H. L., Indiana University and United States of America (2002) *Surveillance Tools for Safer Schools: Final Report*. National Criminal Justice Reference Service.
35. Blossnich, J., and Bossarte, R. (2011) "Low-Level Violence in Schools: Is There an Association Between School Safety Measures and Peer Victimization?" *Journal of School Health*, 81(2), 107–113.
36. Bon, S. C., Faircloth, S. C., and LeTendre, G. K. (2006) "The School Violence Dilemma Protecting the Rights of Students with Disabilities While Maintaining Teachers' Sense of Safety in Schools." *Journal of Disability Policy Studies*, 17(3), 148–157.
37. Bott, S., Morrison, A., and Ellsberg, M. (2005) "Preventing and responding to gender-based violence in middle and low-income countries: a global review and analysis." *World Bank Publications*. Vol. 3618.
38. Boutelle, M. (February 2008) "Uniforms: Are They a Good Fit?" *Education Digest: Essential Readings Condensed for Quick Review*, 73(6), 34–37.
39. Bracy, N. L. (2010) "Circumventing the Law: Students' Rights in Schools with Police." *Journal of Contemporary Criminal Justice*. 26(3). 294–315.
40. Bracy, N. L. (2010) "Student perceptions of high-security school environments." *Youth & Society*.
41. Bradner, E., and Marsh, R. (June 2015) "Acting TSA Director reassigned after screeners failed tests to detect explosives, weapons." CNN. <http://www.cnn.com/2015/06/01/politics/tsa-failed-undercover-airport-screening-tests/>
42. Brady, K. P., Balmer, S., and Phenix, D. (2007) "School—Police Partnership Effectiveness in Urban Schools: An Analysis of New York City's Impact Schools Initiative." *Education and Urban Society*, 39(4), 455–478.
43. Brinkley, C. J., and Saarnio, D. A. (2006) "Involving students in school violence prevention: are they willing to help?" *Journal of School Violence*, 5(1), 93–106.
44. Brown, B. (2006) "Controlling crime and delinquency in the schools: An exploratory study of student perceptions of school security measures." *Journal of School Violence*, 4(4), 105–125.
45. Brown, B. (2006) Understanding and assessing school police officers: A conceptual and methodological comment. *Journal of Criminal Justice*, 34(6), 591–604.

46. Brunner, J. M., and Lewis, D. K. (2008) *Safe & Secure Schools: 27 Strategies for Prevention and Intervention*. Corwin Press.
47. Buck, S., Yurvati, E., and Drake, D., Center for Homicide Research and United States of America. (2013) "Teachers with Guns: Firearms discharges by school teachers, 1980–2012." *Center for Homicide Research*. Retrieved from <http://homicidecenter.org/wp-content/uploads/2013/08/Teachers-with-Guns-RESEARCH-REPORT-FINAL1.pdf>.
48. Burger, L. (18 June 2014) "Can ballistic blankets protect kids from shooters, disasters?" PoliceOne.com. Retrieved 17 September 2015 from <http://www.policeone.com/police-products/tactical/ballistic-shields/articles/7300552-Can-ballistic-blankets-protect-kids-from-shooters-disasters>.
49. Burrow, J. D., and Apel, R. (2008) "Youth behavior, school structure, and student risk of victimization." *Justice Quarterly*, 25(2), 349–380.
50. Burton, S. (5 July 2015) "25 Things People Didn't Know About Bulletproof Vests." *BodyArmor News*. Retrieved 3 December 2015 from <http://www.bodyarmornews.com/bulletproof-vests/>.
51. Cai, G., Dias, J., and Seneviratne, L. (2014) "A survey of small-scale unmanned aerial vehicles: Recent advances and future development trends." *Unmanned Systems*, 2(02), 175–199.
52. *Campus Safety Magazine* (2015) "University of Arkansas Bans Drones on Campus." Retrieved 3 September 2015 from http://www.campussafetymagazine.com/article/univ._of_arkansas_bans_drones_on_campus.
53. *Campus Safety Magazine* (2016) "What's Next for Physical Security Information Management Systems?" http://www.campussafetymagazine.com/article/an_expert_gives_reflections_and_predictions_on_the_psim_world?utm_source=newsletter&utm_medium=email&utm_campaign=productnews#
54. Caplan, J. M., Kennedy, L. W., and Petrossian, G. (2011) "Police-monitored CCTV cameras in Newark, NJ: A quasi-experimental test of crime deterrence." *Journal of Experimental Criminology*. 7(3), 255–274.
55. Carney, S. (2014) "Managing Security Technology: Should You Adopt a VMS or PSIM?" *Campus Safety*. Retrieved from <http://www.campussafetymagazine.com/article/The-Sum-of-All-Security>.
56. Casella, R. (2003) "The false allure of security technologies." *Social Justice*. 30(3). 82–93.
57. Center for the Study and Prevention of Violence (2000) Retrieved 24 September 2015 from <http://www.colorado.edu/cspv/publications/factsheets/safeschools/FS-SC04.pdf>.
58. Centers for Disease Control and Prevention (2014). *Understanding School Violence: Fact Sheet*. MMWR Surveillance Summaries, 63, SS-4. Retrieved 24 September 2015 from www.cdc.gov/mmwr/pdf/ss/ss6304.pdf.
59. Chilcott, T., and Odgers, R. (2009) "Government can do more on school violence." Retrieved from <http://www.couriermail.com.au/>.

60. Chipley, M. et al. (2012) *"Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings. Buildings and Infrastructure Protection Series."* FEMA-428/BIPS-07/January 2012. Edition 2. U.S. Department of Homeland Security (2012).
61. Cho, D. (2014) "Maryland school district to start monitoring students' social media posts with new software." WJLA News. Retrieved 1 September 2015 from <http://wjla.com/news/local/maryland-school-district-to-start-monitoring-students-social-media-posts-with-new-software-105814>.
62. Christle, C. A., Jolivette, K., and Nelson, C. M. (2005) "Breaking the school to prison pipeline: Identifying school risk and protective factors for youth delinquency." *Exceptionality*, **13**(2), 69–88.
63. Cisneros, C. (2010) *Two local districts using student tracking devices*. Retrieved 24 September 2015 from <http://abc13.com/archive/7717793/>.
64. Clark, J. (October 2012) "What is a Man-trap and Do You Need One?" *The Data Center Journal*. <http://www.datacenterjournal.com/what-is-a-man-trap-and-do-you-need-one/>.
65. Clark, M. D. (4 September 2015) "State changes may force Kings to drop security device." Cincinnati.com. Retrieved 4 December 2015 from <http://www.cincinnati.com/story/news/education/2015/09/04/school-security-clash/71702998/>.
66. Clark, N. (2013) "Education in Mexico." *World Education News and Reviews*. Retrieved from <http://wenr.wes.org/2013/05/wenr-may-2013-an-overview-of-education-in-mexico/>.
67. Clarke, R. (2008) "Improving Street Lighting to Reduce Crime in Residential Areas." *Problem-Oriented Guides for Police Series No. 8*, p. 11.
68. Clifton, K. J. and Kremer-Fults, K. (July 2007) "An Examination of the environmental attributes associated with pedestrian-vehicle crashed near public schools." *Accident Analysis and Prevention*, **39**(4), 708–15.
69. Cogan, A. (2015) "Schools become a safe haven from violence." Retrieved from <https://www.mercycorps.org/articles/colombia/school-becomes-safe-haven-violence>.
70. Cohn, J. P. (2006) "Keeping an eye on school security: The Iris Recognition Project in New Jersey schools." *NIJ Journal*, 254, 12–15.
71. *Computerworld* (12 February 2013) "Hacker broadcasts emergency zombie apocalypse warning on TV station in Montana." Retrieved 2 September 2015 from <http://www.computerworld.com/article/2474427/cybercrime-hacking/hacker-broadcasts-emergency-zombie-apocalypse-warning-on-tv-station-in-montana.html>.
72. Congress of the U.S. Office of Technology Assessment (July 1991) "Technology Against Terrorism: The Federal Effort," Appendix B.
73. Connor, T. (21 August 2013) "Bulletproof school supplies get low grades from safety experts." NBC News. Retrieved 4 September 2015 from <http://www.nbcnews.com/news/other/bulletproof-school-supplies-get-low-grades-safety-experts-f6C10963127>.
74. Cook, C., and Shinkle, D. (2012) National Conference of State Legislatures Transportation Review, *School Bus Safety*. http://www.ncsl.org/documents/transportation/schoolbus_tranrev0810.pdf

75. Coon, J. K. (2007) *Security Technology in U.S. Public Schools*. LFB Scholarly Publishing, LLC.
76. Cornell, D. G. (2009) "The Virginia model for student threat assessment." *Workshop at the XIV Workshop Aggression*. Freie Universität, Berlin, Germany.
77. Cornell, D. G., and Mayer, M. J. (2010) "Why do school order and safety matter?" *Educational Researcher*, **39**(1), 7–15.
78. Csere, M. (2013) "School security in Israel." Retrieved from <https://www.cga.ct.gov/2013/rpt/2013-R-0119.htm>.
79. *Daily Sabah* (2014) "Millions back to school with less burden, more security." Retrieved from <http://www.dailysabah.com/education/2014/09/16/millions-back-to-school-with-less-burden-more-security>.
80. Davidson, J., and Martellozzo, E. (2013) "Exploring young people's use of social networking sites and digital media in the Internet safety context: a comparison of the UK and Bahrain." *Information, Communication & Society*, **16**(9), 1456–1476.
81. De Janvry, A., Finan, F., Sadoulet, E., and Vakis, R. (2006) "Can conditional cash transfer programs serve as safety nets in keeping children at school and from working when exposed to shocks?" *Journal of Development Economics*, **79**(2), 349–373.
82. DeAngelis, K. J., and Brent, B. O. (2012) "Books or Guards? Charter School Security Costs." *Journal of School Choice*, **6**(3), 365–410.
83. DeAngelis, K. J., Brent, B. O., and Ianni, D. (2011) "The hidden cost of school security." *Journal of Education Finance*, **36**(3), 312–337.
84. Deb, S., and Walsh, K. (2012) "Impact of physical, psychological, and sexual violence on social adjustment of school children in India." *School Psychology International*, **33**(4), 391–415.
85. Defense Science Board (August 2012) *Task Force Report: Predicting Violent Behavior*. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. <http://www.acq.osd.mil/dsb/reports/PredictingViolentBehavior.pdf>.
86. Desourdis, Jr., R. I., McCoskey, J., O'Brien, M., and Wyglinski, A. M. "Secure Targetable Digital Television Datacast." Retrieved 11 December 2015 from <http://www.spectrarep.com/nationaldistributionwhitepaper.pdf>.
87. Desourdis, Jr., R. I., Vest, K. F., O'Brien, M., and Mulholland, D. J. (November 2011). "Digital television for homeland security: Broadband datacast for situational awareness and command coordination." *IEEE International Conference on Technologies for Homeland Security*. 33–42.
88. Dick, W. (2016) "Schools work to cope with threat of shootings." Retrieved from <http://www.dw.com/en/schools-work-to-cope-with-threat-of-shootings/a-15978539>.
89. *Digest of Education Statistics* (2012) Retrieved 24 September 2015 from <http://nces.ed.gov/programs/digest/d12/>.
90. Dinkes, R., Cataldi, E. F., Kena, G., and Baum, K. (2006) *Indicators of School Crime and Safety: 2006*. NCES 2007-003. National Center for Education Statistics.

91. Donaghey, M. J. (2013) *Protecting our future: developing a national school security standard*. Doctoral dissertation, Monterey, California: Naval Postgraduate School.
92. Dorn, C. (2007). "Innocent targets: When terrorism comes to school."
93. Dorn, M., Shepherd, S., Satterly, S. and Dorn, C. (2014) Safe Havens International, Inc. *Staying Alive: How to Act Fast and Survive Deadly Encounters*. Barron's.
94. Dumbaugh, E., and Frank, L. (2007) "Traffic safety and safe routes to schools: synthesizing the empirical evidence." *Transportation Research Record: Journal of the Transportation Research Board*, **2009**(1), 89–97
95. Dunne, M., Humphreys, S., and Leach, F. (2006) "Gender violence in schools in the developing world." *Gender and Education*, **18**(1), 75–98.
96. Dworkin, A. G., Haney, C. A., and Telschow, R. L. (1988) "Fear, victimization, and stress among urban public school teachers." *Journal of Organizational Behavior*, **9**(2), 159–171.
97. Earl, J. (2006) "Exterior lighting for safety and security." *Buildings*.
<http://www.buildings.com/article-details/articleid/3084/title/exterior-lighting-for-safety-and-security.aspx>.
98. Education International (2013) "Education in crisis: Afghanistan." Retrieved from <http://www.educationincrisis.net/country-profiles/asia-pacific/item/551-afghanistan>.
99. Education Policy and Data Center (2014) "National education profile: Central African Republic." Retrieved from http://www.epdc.org/sites/default/files/documents/EPDC%20NEP_Central%20African%20Republic.pdf.
100. *Education Week* (2013) "School safety legislations since Newtown." Retrieved 24 September 2015 from <http://www.edweek.org/ew/section/multimedia/school-safety-bills-since-newtown.html>.
101. Eisenbraun, K. D. (2007) "Violence in schools: Prevalence, prediction, and prevention." *Aggression and Violent Behavior*, **12**(4), 459–469.
102. Elias, B. (23 April 2009) "Airport Passenger Screening: Background and Issues for Congress." *Congressional Research Services Report for Congress*.
<https://www.fas.org/sgp/crs/homesec/R40543.pdf>.
103. Ellison, Q. (2014) "School officials to monitor students' social media use." *Sylva Herald*. Retrieved from http://www.thesylvaherald.com/breaking_news/article_a04a7136-11b2-11e4-9e49-001a4bcf6878.html.
104. ElMeShad, S. (2012) "Egypt's school system: Taking a look at schools, their curricula, and accreditation." *Egypt Independent News*. Retrieved from <http://www.egyptindependent.com/news/egypt-s-school-system-taking-look-schools-their-curricula-and-accreditation>.
105. Nation's Encyclopedia (2014) Columbia: Education. Retrieved 24 March 2016 from <http://www.nationsencyclopedia.com/Americas/Columbia-EDUCATION.html>

106. Ergenbright, C. et al. (2012) *Defeating the Active Shooter: Applying Facility Upgrades in Order to Mitigate the Effects of Active Shooters in High-Occupancy Facilities*, U.S. Naval Postgraduate School.
107. Eyewitness News ABC-7 New York (29 September 2014) "Gun Found On Grounds of Long Island Middle School." Retrieved 4 November 2015 from <http://abc7ny.com/education/unloaded-gun-found-on-grounds-of-li-middle-school/328893/>
108. Farley, T. A. et al.(2007) "Safe play spaces to promote physical activity in inner-city children: results from a pilot study of an environmental intervention." *American Journal of Public Health*, **97**(9), 1625.
109. Federal Aviation Administration (1 June 2015) "Small UAS Notice of Proposed Rulemaking (NPRM)." Retrieved 3 September 2015 from <http://www.faa.gov/uas/nprm/>.
110. Federal Bureau of Investigation (16 September 2013) "A Study of Active Shooter Incidents in the United States Between 2000 and 2013."
111. Federal Emergency Management Agency (2013) "Local Mitigation Planning Handbook." Washington, DC.
112. Federal Emergency Management Agency (2013) Online training: IS-362.A: Multi-Hazard Emergency Planning for Schools, Lesson 4. Retrieved from <https://emilms.fema.gov/IS362a/SMHP0104summary.htm>.
113. Federal Emergency Management Agency. Retrieved 5 October 2015 from www.fema.gov/national-incident-management-system.
114. Federal Aviation Administration. "Overview of Small UAS Notice of Proposed Rulemaking." Retrieved 30 November 2015 from https://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf.
115. Fennelly, L., and Perry, M. (2014) *The Handbook for School Safety and Security: Best Practices and Procedures*. Butterworth-Heinemann.
116. Ferguson, C. J., Coulson, M., and Barnett, J. (2011) "Psychological profiles of school shooters: Positive directions and one big wrong turn." *Journal of Police Crisis Negotiations*, **11**(2), 141–158.
117. Fiel, P. V., Sr. (December 2014) "Maintaining a Secure Environment." *School Planning and Management*.
118. Finklestein, D. (January 2013) *School Business Affairs*. Retrieved from http://asbo.org/images/downloads/Articles/sba_jan2013_picture_this.pdf
119. Fletcher, G. H., and Jensen, R. C. (2008) "Converge Your Resources: Linking Physical Security and Cyber Security Methods Can Maximize a District's Safety Efforts." *Technological Horizons in Education*, **35**(10), S3.

120. Florida Department of Education (2016) "School Environmental Safety Incident Reporting (SESIR) System," *Appendix P: Definitions for Incident Reporting*. Retrieved 29 March 2016 from <http://www.fldoe.org/schools/safe-healthy-schools/safe-schools/sesir-discipline-data/discipline-incident-data/sesir-discipline-data-collection-syste.html>.
121. Focht-New, G., Clements, P. T., Barol, B., Faulkner, M. J., and Service, K. P. (2008) "Persons with developmental disabilities exposed to interpersonal violence and crime: Strategies and guidance for assessment." *Perspectives in Psychiatric Care*, **44**(1), 3–13.
122. Foreign Credits, Inc. (2012) "Education data base: Education system in the Central African Republic." Retrieved from <http://www.classbase.com/countries/Central-African-Republic/Education-System>.
123. Freeman, J. (February 2015) "North Penn School District Gears-Up To Make Schools Safer." *The Reporter*. <http://www.thereporteronline.com/social-affairs/20150216/north-penn-school-district-gears-up-to-make-schools-safer>.
124. Funck, G. (1999) "The Building Blocks of School Security." *School Business Affairs*, **65**(6), 29–31.
125. Galand, B., Lecocq, C., and Philippot, P. (2007) School violence and teacher professional disengagement. *British Journal of Educational Psychology*, **77**(2), 465–477.
126. Garcia, C. A. (2003) "School safety technology in America: Current use and perceived effectiveness." *Criminal Justice Policy Review*, **14**(1), 30–54.
127. Garriss, K. (4 July 2014) Intelligence Based Software Helps Police Predict Crimes. Whag.com. Retrieved from <http://www.your4state.com/news/news/intelligence-based-software-helps-police-predict-crimes>
128. Gastic, B. (2010) "Metal detectors and feeling safe at school." *Education and urban society*. 43(3), 486–98, doi:10.1177/0013124510380717.
129. Gastic, B., and Johnson, D. (2014) "Disproportionality in Daily Metal Detector Student Searches in U.S. Public Schools." *Journal of School Violence*, (ahead of print), 1–17.
130. Global Coalition to Protect Education from Attack (2013) "Country Profiles: Colombia." Retrieved from <http://www.protectingeducation.org/country-profile/colombia>.
131. Global Coalition to Protect Education from Attack (2013) "Country Profiles: Côte d'Ivoire." Retrieved from <http://www.protectingeducation.org/country-profile/colombia>.
132. Global Coalition to Protect Education from Attack (2013) "Country Profiles: Democratic Republic of the Congo." Retrieved from <http://www.protectingeducation.org/country-profile/democratic-republic-congo>.
133. Global Coalition to Protect Education from Attack (2013) "Country Profiles: India." Retrieved from <http://www.protectingeducation.org/country-profile/india>.
134. Global Coalition to Protect Education from Attack (2013) "Country Profiles: Mexico." Retrieved from <http://www.protectingeducation.org/country-profile/mexico>.

135. Global Coalition to Protect Education from Attack (2013) "Country Profiles: Turkey Retrieved from <http://www.protectingeducation.org/country-profile/turkey>.
136. Goldfine, S. (2014) "Knowing these 17 emerging security technology trends." *Campus Safety*. Retrieved 24 September 2015 from http://www.campus safetymagazine.com/article/know_these_17_emerging_security_technology_trends/P2.
137. Gottfredson, G. D., and Gottfredson, D. C. (2001) "What schools do to prevent problem behavior and promote safe environments." *Journal of Educational and Psychological Consultation*, **12**(4), 313–344.
138. Grave-Lazi, L. (2015) "Education ministry updates guidelines for dealing with violent incidents in schools." *The Jerusalem Post*. Retrieved from <http://www.jpost.com/Israel-News/Education-Ministry-updates-guidelines-for-dealing-with-violent-incidents-in-schools-395833>.
139. Green, M. W. (September 1999) *The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies*. DOJ Office of Justice Programs and NIJ. Retrieved from https://www.ncjrs.gov/school/ch3a_2.html.
140. Greene, M. B. (2005) "Reducing violence and aggression in schools." *Trauma, Violence, & Abuse*, **6**(3), 236–253.
141. Griffin, A. (2015) "Schools use social media monitoring software to watch students." *The Independent*. Retrieved from <http://www.independent.co.uk/life-style/gadgets-and-tech/news/schools-use-social-media-monitoring-software-to-watch-students-10288541.html>
142. Guderian, B. (2004) "Wireless telephones help schools increase communications, decrease safety risks." *Technological Horizons in Education*, **31**(8), 28.
143. Guilbert, K. (2015) "Violence, fear in northern Mali deprive children of education." Reuters Editorial. Retrieved from <http://www.reuters.com/article/us-mali-education-idUSKBN0U100D20151218>.
144. Gurken, M. (2015) "As Turkey's students head back to class, many fear escalating violence." Retrieved from <http://www.al-monitor.com/pulse/en/originals/2015/09/turkey-pkk-mounting-fear-of-clashes-with-schools-opening.html#>.
145. Halloran, E. (4 May 2013) "Bulletproof Whiteboards and the Marketing of School Safety." National Public Radio. Retrieved 11 April 2016 from <http://www.soundcheck.wnyc.org/story/291458-bulletproof-whiteboards-and-the-marketing-of-school-safety/>.
146. Hankin, A., Hertz, M., and Simon, T. (2011) "Impacts of Metal Detector Use in Schools: Insights from 15 Years of Research." *Journal of School Health*, **81**(2), 100–106.
147. Hanover Research (2013). District Administration Practice. *Best Practices in School Security: Prepared for School XYZ*.
148. Hanover Research (2013) *School Fencing: Benefits and Disadvantages*. <http://www.wssca.org/pdf/School%20Fencing-%20Benefits%20and%20Disadvantages.pdf>.

149. Harder, S. (2015) "Lighting for Safety and Security." <http://www.darksksociety.org/resources.cfm?page=handouts&scope=all>
150. Harman, K., and Messner, W. K. (October 2012) "Outdoor perimeter security sensors: A forty-year perspective." *IEEE, 2012 IEEE International Carnahan Conference on Security Technology (ICCSST)*, 1–9.
151. Harney, R. (2005) *Combat Systems Vol. 1: Sensors*, Chapter 14: Imaging and Image-based Perception. <http://www.nps.navy.mil/se/harney/cbt1ch14.pdf>.
152. Harrauld, J., and Jefferson, T. (January 2007) "Shared situational awareness in emergency management mitigation and response." *IEEE, 40th Annual Hawaii International Conference on System Sciences*, 23–23.
153. Hattersley-Gray, Robin (7 June 2010) "How to Detect a Concealed Weapon." *Campus Safety Magazine*. <http://www.campussafetymagazine.com/article/how-to-detect-a-concealed-weapon>
154. Hermann, M. A., and Remley Jr, T. P. (2000) "Guns, violence, and schools: The results of school violence-litigation against educators and students shedding more constitutional rights at the school house gate." *Loy. L. Rev.*, **46**, 389.
155. Hernandez, D., Floden, L., and Bosworth, K. (2010) "How safe is a school? An exploratory study comparing measures and perceptions of safety." *Journal of School Violence*, **9**(4), 357–374.
156. Hevia, J. (2013). *Impediments to U.S. Educational and Public Institutions Ameliorating the Mass Shooting Epidemic with Effective State-of-the-Art Security Solutions and the Introduction of a School Access-Control Vulnerability Index (S.A.V.I.) Audit and Certification Process, As a Solution*. Napco Security Technologies, Inc.
157. Hibbert, C. (2015) "Are schools wasting limited money on questionable security vendor products?" National School Safety and Security Services. Retrieved 24 September 2015 from <http://www.schoolsecurity.org/2015/02/schools-wasting-limited-money-questionable-security-vendor-products/>.
158. Higgins, S., Hall, E., Wall, K., Woolner, P., and McCaughey, C. (2005) "The impact of school environments: A literature review." Design Council.
159. Hinduja, S., and Patchin, J. W. (2012) "Cyberbullying: Neither an epidemic nor a rarity." *European Journal of Developmental Psychology*, **9**(5), 539–543.
160. Humanitarian News and Analysis (2011) "DRC: Millions miss out on basic education." Retrieved from <http://www.irinnews.org/report/94196/drc-millions-miss-out-on-basic-education>.
161. Hunt, S. (2010). "Physical security information management (PSIM): The basics." *CSO*. <http://www.csoonline.com/article/2126002/metrics-budgets/physical-security-information-management--psim---the-basics.html>
162. Idaho State University (24 October 2014) "Idaho State University Lockdown Procedures." Retrieved 3 December 2015 from <http://www.isu.edu/pubsafe/errp/LockdownProcedures.pdf>.

163. Ihde, A., and Taylor, S (1 June 2015). *Trip Report of the School Safety Technology Initiative Site Visit to Carroll County School Security Office, 8 May 2015*. JHU/APL. AOS-15-0577.
164. Illuminating Engineering Society of North America (2003) *Guideline for Security Lighting for People, Property, and Public Spaces (G-1-03)*.
165. International Code Council (2012) *International Building Code*. Retrieved from <http://publicecodes.cyberregs.com/icod/ibc/index.htm>.
166. Ismayilov, S. (2016) "Blast attack in Turkish elementary school, 5 students injured." Retrieved from <http://report.az/en/region/blast-attck-in-turkish-elementary-school-5-students-injured/>.
167. Israel Ministry of Education (2013) "The Israeli Education System Strives to Protect Its Schools and Students from Terror." Retrieved from http://www.education.gov.il/children/page_54.htm.
168. Jackson, A. (2002) "Police-SROs' and students' perception of the police and offending." *Policing: An International Journal of Police Strategies & Management*, **25**(3), 631–650.
169. Jalonick, M. C. (5 July 2015) "How drones could replace workers on American Farms." *Associated Press*. Retrieved 2 September 2015 from <http://www.pbs.org/newshour/rundown/farmers-frustrated-lack-drone-access/>.
170. James, N., and McCallion, G. (2013) *School resource officers: Law enforcement officers in schools*. Congressional Research Service.
171. Jennings, W. G., Khey, D. N., Maskaly, J., and Donner, C. M. (2011) "Evaluating the relationship between law enforcement and school security measures and violent crime in schools." *Journal of Police Crisis Negotiations*, **11**(2), 109–124.
172. Jimerson, S. R., and Furlong, M. J. (2006) *The handbook of school violence and school safety: From research to practice*.
173. Jimerson, S., Brown, J., Stifel, S., and Rudeman, M. (2012) "World report on violence and health: International insights." *Handbook of School Violence and School Safety*. Retrieved from https://books.google.com/books?id=f__FBQAAQBAJ&pg=PT383&lpg=PT383&dq=egypt+school+safety&source=bl&ots=o5vDsFqly-&sig=3ueTJQPKavMFRCpoc84OIHiGSWI&hl=en&sa=X&ved=0ahUKEwiDjZSeosjKAhXF6iYKHUb8CtA4ChDoAQhBMAY#v=onepage&q&f=false
174. Johnson, W. S. (2010) *Analyses of the impact of school uniforms on violence in North Carolina public high schools*. ProQuest LLC (EdD Dissertation, East Carolina University).
175. Jones, S. E., Axelrad, R., and Wattigney, W. A. (2007) "Healthy and safe school environment, part II, physical school environment: results from the School Health Policies and Programs Study – 2006." *Journal of School Health*, **77**(8), 544–556.
176. Juvonen, J. (2001) *School violence: Prevalence, fears, and prevention*. RAND Corporation. Santa Monica, CA.

177. Kaiser, L. (2013) "Tackling school safety through design." *Architectural Record*. Retrieved 24 September 2015 from <http://archrecord.construction.com/news/2013/02/130214-Tackling-Safety-Through-Design.asp>.
178. Kaye, J., Hill, R., and Goetz, B. (2013) *School Emergency Management: A Practical Approach to Implementation*. Polimedia Publishing.
179. Kelly, K. (28 October 2015) "Look Out for Camera Drone Integration in 2015 on College Campuses." *Campus Safety Magazine*. Retrieved 3 September 2015 from http://www.campusafetymagazine.com/article/look_out_for_camera_drone_integration_in_2015_on_college_campuses.
180. Kerns, A. J., Shepard, D. P., Bhatti, J. A., and Humphreys, T. E. (2014) "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, **31**(4), 617–636.
181. Khoury-Kassabri, M., Astor, R. A., and Benbenishty, R. (2009) "Middle Eastern Adolescents' Perpetration of School Violence Against Peers and Teachers A Cross-Cultural and Ecological Analysis." *Journal of Interpersonal Violence*, **24**(1), 159–182.
182. Kiernan Coon, J., and Travis III, L. (2012) "The role of police in public schools: a comparison of principal and police reports of activities in schools." *Police Practice and Research*, **13**(1), 15–30.
183. Kim, J. H., Bailey, S., Erkut, S., Aoudeh, N., and Ceder, I. (2003) *Unsafe schools: a literature review of school-related gender-based violence in developing countries*.
184. King, L. (30 April 2015) "Nepal Earthquake Relief And The Urgent Boost From Drones." *Forbes*. Retrieved 2 September 2015 from <http://www.forbes.com/sites/looking/2015/04/30/nepal-earthquake-drones-relief-aid/>.
185. Kitsantas, A., Ware, H. W., and Martinez-Arias, R. (2004) "Students' perceptions of school safety: Effects by community, school environment, and substance use variables." *The Journal of Early Adolescence*, **24**(4), 412–430.
186. Knoke, M. E. (2007) Managing Editor, *Protection of Assets Manual*. Volume III, Section 19. ASIS International.
187. Komola, T. (2015) "Is PSIM Right for Your Campus?" *Campus Safety*. Retrieved from http://www.campusafetymagazine.com/article/is_psim_right_for_your_campus.
188. Kondrasuk, J. N. et al. (2005) "Violence affecting school employees." *Education*, **125**(4), 638.
189. Krone, J. (13 August 2013) "10 Reasons To Switch from Analog Cameras and DVRs to IP Cameras and NVRs." *Business Solutions*.
190. Kuenstle, M. W., and Clark, N. (2003) *Florida Safe School Design Guidelines: Strategies to Enhance Security and Reduce Vandalism*. Florida Department of Education, Office of Education Facilities.
191. Kuepers, J. (14 August 2015) *Security Today*. <https://security-today.com/articles/2015/08/14/integrating-multi-use-school-id-cards.aspx>
192. LaBarre, E. D. et al. (2013) "Multi-scale testing techniques for carbon nanotube augmented Kevlar." *2013 Annual Conference on Experimental and Applied Mechanics*, 3–5 June 2013, 59–68.

193. Lacey, Kylie (2014) District Administration. "The Business of School Visitor Management Systems: Computerized kiosks can help balance safety and convenience."
<http://www.districtadministration.com/article/business-school-visitor-management-systems>.
194. Lacoe, J. R. (2 March 2012) "Too Scared to Learn? The Academic Consequences of Feeling Unsafe at School." Robert F. Wagner Graduate School of Public Services, New York University.
Retrieved 4 September 2015 from
http://www.aefpweb.org/sites/default/files/webform/Lacoe_School%20Safety_3.2012.pdf.
195. Lambeck, L. (2014) "Schools Mull Computer Background Checks on Visitors." *CT Post*. Retrieved from <http://www.ctpost.com/local/article/Schools-mull-computer-background-checks-on-5817433.php>.
196. Lambert, R., and McGinty, D. (2002) "Law enforcement officers in schools: Setting priorities." *Journal of Educational Administration*, **40**(3), 257–273.
197. Lapriore, E. (2005) "Grade school violence a global problem: Astor finds in largest-ever study on child victimization in schools." Retrieved from <https://sowkweb.usc.edu/news/grade-school-violence-global-problem-astor-finds-largest-ever-study-child-victimization-schools>.
198. Laurie, E. (2010) Learn without fear: Campaign progress report. Retrieved from <http://resourcecentre.savethechildren.se/library/learn-without-fear-campaign-progress-report>.
199. Leila, R. (2015) "Dealing with school violence." Retrieved from <http://weekly.ahram.org.eg/News/10954/24/Dealing-with-school-violence.aspx>.
200. Le Mat, M. (2013) "Addressing sexual violence in schools: Perspectives from teachers and students in a secondary school in Addis Ababa, Ethiopia." Retrieved from <https://educationanddevelopment.files.wordpress.com/2013/11/thesis2-marielle-le-mat.pdf>.
201. Lenhart, A., Smith, A., Anderson, M., Duggan, M., Perrin, A. (August 2015) "Teens, Technology and Friendships." Pew Research Center. Retrieved from <http://www.pewInternet.org/2015/08/06/teens-technology-and-friendships/>.
202. Leonard, R. C., Salande, J. P., and Mamoulides, J. M. (2008) U.S. Patent Application 12/012,134.
203. Leuschner, V. et al. (2011) "Prevention of homicidal violence in schools in Germany: the Berlin leaking project and the Networks Against School shootings Project (NETWASS)." *New Directions for Youth Development*, **2011**(129), 61–78.
204. Lewis, B. (2014). "Alabama schools leave digital footprint." Retrieved 24 September 2015 from <https://www.schoolsafetyinfo.org/alabama.html>.
205. Lincke, S. (2015) "Designing Physical Security." *Security Planning*, 159–170. Springer International Publishing.
206. Lindle, J. C. (2008) "School Safety Real or Imagined Fear?" *Educational Policy*, **22**(1), 28–44.
207. Liu, S., and Silverman, M. (2001) "A practical guide to biometric security technology." *IT Professional*, **3**(1), 27–32.

208. Lohman, J., and Shepard, A. (2006) *School Security Technologies*. Connecticut Office of Legislative Research 2006-R-0668. Retrieved 24 September 2015 from <http://www.cga.ct.gov/2006/rpt/2006-R-0668.htm>.
209. Madico Technical Resources. "FAQ's – What is window film?" Retrieved 19 November 2015 from <http://www.madico.com/window-film/technical-resources/faqs/>.
210. Magee, Maureen (11 January 2015) *The San-Diego Union Tribune*. Retrieved from <http://www.sandiegouniontribune.com/news/2015/jan/11/fences-spark-discussion-on-school-safety-effort/>.
211. Marginson, S., Nyland, C., Sawir, E., and Forbes-Mewett, H. (2010) *International Student Security*. Retrieved from <https://books.google.com/books?hl=en&lr=&id=GJtId88rGp0C&oi=fnd&pg=PR8&dq=student+security+eastern+europe&ots=uz1hNYabil&sig=rUYO-yPD9epe0pPRQgt-xNeC0yA#v=onepage&q=student%20security%20eastern%20europe&f=false>.
212. Martin, Claire (27 December 2014) "Out of Tragedy, a Protective Glass for Schools." *The New York Times*. Retrieved 9 November 2015 from http://www.nytimes.com/2014/12/28/technology/out-of-tragedy-a-protective-glass-for-schools.html?_r=0.
213. Maxwell, L. E. (2000) "A safe and welcoming school: What students, teachers, and parents think." *Journal of Architectural and Planning Research*.
214. May, D., Hart, T., and Ruddell, R. (2011) "School resource officers in financial crisis: Which programs get cut and why." *Journal of Police Crisis Negotiations*, 11(2), 125–140.
215. McAdams III, C. R., and Foster, V. A. (2008) "Voices from 'The Front' How Student Violence Is Changing the Experience of School Leaders." *Journal of School Violence*, 7(2), 87–103.
216. McCarthy, M. R., and Soodak, L. C. (2007) "The politics of discipline: Balancing school safety and rights of students with disabilities." *Exceptional Children*, 73(4), 456–474.
217. McClean, D. (2015) "Action agreed on safe schools." United Nations Office for Disaster Risk Reduction. Retrieved from <https://www.unisdr.org/archive/46050>.
218. McMahon, K. (2014) "What does the PSIM market have to offer." *Security News Desk*. <http://www.securitynewsdesk.com/psim-market-offer/>.
219. McMahon, S. D. et al. (2014) "Violence directed against teachers: Results from a national survey." *Psychology in the Schools*, 51(7), 753–766.
220. Melde, C., and Esbensen, F. A. (2009) "The Victim-Offender Overlap and Fear of In-School Victimization A Longitudinal Examination of Risk Assessment Models." *Crime & Delinquency*, 55(4), 499–525.
221. Merkow, M. S., and Breithaupt, J. (2014) *Information Security: Principles and Practices*. Pearson Education.
222. Minnesota Department of Public Safety (2011) *Minnesota Comprehensive School Safety Guide*. Minnesota School Safety Center Program.

223. Mitchell, J. T., and Everly, G. S. (2000) "Critical incident stress management and critical incident stress debriefings: Evolutions, effects and outcomes." *Psychological debriefing: Theory, practice, and evidence*, 71–90.
224. Monahan, J., Steadman, H., Silver, E., Appelbaum, P., Robbins, P., Mulvey, E., Roth, L., Grisso, T., and Banks, S. (2001). *Rethinking Risk Assessment: The MacArthur Study of Mental Disorder and Violence*. New York: Oxford University Press.
225. Morton, Jennie (March 2011) "Vehicle Barriers for Facility Protection." Buildings.Com. <http://www.buildings.com/article-details/articleid/11706/title/vehicle-barriers-for-facility-protection.aspx>.
226. Mowen, T. J. (2013) "Parental Involvement in School and the Role of School Security Measures." *Education and Urban Society*.
227. Mowen, T. J., and Parker, K. F. (2014) "Minority threat and school security: Assessing the impact of Black and Hispanic student representation on school security measures." *Security Journal*.
228. Na, C., and Gottfredson, D. C. (2013) "Police officers in schools: Effects on school crime and the processing of offending behaviors." *Justice Quarterly*, **30**(4), 619–650.
229. Nagel, D. (2014) "School Physical Security Spending To Top \$1.1 Billion Within 4 Years." Retrieved from <https://thejournal.com/articles/2014/11/19/campus-physical-security-spending-to-top-1.1-billion-within-4-years.aspx>.
230. Nance, J. P. (2014) "School Surveillance and the Fourth Amendment." *Wis. L. Rev.*, **79**.
231. Nance, J. P. (2013) "Students, Security, and Race." *63 Emory L. J.* 1.
232. Naples, K., and Zieller, C. (17 September 2015) "Bullet found lodged in Hartford school window pane," Eyewitness News 3. Retrieved 9 November 2015 from <http://www.wfsb.com/story/30057136/bullet-found-lodged-in-hartford-school-window-pane>.
233. National Association of State Boards of Education (2009) "Safe and Drug Free Schools." Retrieved 24 September 2015 from http://www.nasbe.org/healthy_schools/hs/bytopics.php?topicid=3130.
234. National Center for Education Statistics. (2013) "Status of rural schools." Retrieved 24 September 2015 from http://nces.ed.gov/programs/coe/indicator_tla.asp.
235. National Center for Education Statistics (2014) "Public high schools ranked by enrollment." Retrieved 24 September 2015 from <http://high-schools.com/report/public-high-schools-list.html>.
236. National Center for Education Statistics, Institute of Education Sciences, Bureau of Justice Statistics (June 2014). *Indicators of School Crime and Safety: 2013*. NCES 2014-042 NCJ 243299. Table 20.1, "Percentage of public and private schools with various safety and security measures, by school level: 2003–04, 2007–08, and 2011–12."
237. National Center for Education Statistics (2015) "Public School Safety and Discipline: 2013–2014." <http://nces.ed.gov/pubs2015/2015051.pdf>.
238. National Clearinghouse for Educational Facilities (2008) "Improving School Access Control." Retrieved from <http://www.ncef.org/pubs/accesscontrol.pdf>.

239. National Clearinghouse for Educational Facilities (2008) "Mitigating hazards in school facilities." Retrieved 24 September 2015 from http://www.ncef.org/pubs/pubs_html.cfm?abstract=mitigating2.
240. National Clearinghouse for Educational Facilities (July 2010) "School Security Technologies." http://www.ncef.org/pubs/security_technologies.pdf.
241. National Conference of State Legislators (26 August 2015) "Current Unmanned Aircraft State Law Landscape." Retrieved 3 September 2015 from <http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx>.
242. National Crime Prevention Council (2003) *School Safety and Security Toolkit: A Guide for Parents, Schools, and Communities*. Washington, DC.
243. National Criminal Justice Technology Research, Test, and Evaluation (RT&E) Center (2015) *School Safety and Security Technology: Literature Review*. Version 1.0.
244. National Fire Prevention Association Research and Reports (2014). *Workshop on School Safety, Codes and Security*. Final Report.
245. National Fire Prevention Association (2015) *NFPA 805 Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plant*. Section 1.2. Quincy MA.
246. National Institute for Occupational Safety and Health (2004) "Safety checklist programs for schools." Retrieved 24 September 2015 from <http://www.cdc.gov/niosh/docs/2004-101/>.
247. National Law Enforcement and Corrections Technology Center for the National Institute of Justice (October 1998) "Selection and Application Guide to Police Body Armor," Appendix C. Retrieved 17 September 2015 from <https://www.ncjrs.gov/pdffiles/169587.pdf>.
248. National School Safety and Security Services (2015) *School Security Equipment and Technology*. Retrieved 24 September 2015 from <http://www.schoolsecurity.org/category/school-security-equipment-technology/>.
249. National School Safety Center (2010) *Schools and Readiness*. <http://www.schoolsafety.us/free-resources/schools-and-readiness>.
250. National Security Agency, Information Assurance Solutions Group (STE 6737). *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments*. Retrieved 28 October 2015 from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf.
251. Neshet, T. (2012) "Study: School violence in Israel; down 25%." Retrieved from <http://www.haaretz.com/study-school-violence-in-israel-down-by-25-1.414026>.
252. Ness, D., and Lin, C. L. (2015) *International Education: An Encyclopedia of Contemporary Issues and Systems*. Routledge.
253. Netshitahame, N. E., and Van Vollenhoven, W. J. (2006) "School safety in rural schools: Are schools as safe as we think they are?" *South African Journal of Education*, **22**(4), 313–318.

254. Nickerson, A. B., and Martens, M. P. (2008) "School violence: Associations with control, security/enforcement, educational/therapeutic approaches, and demographic factors." *School Psychology Review*.
255. Niesse, Mark, and Burnette, Daarel II (March 2013) "School Administrators Reevaluate Use of Metal Detectors." *The Atlanta Journal-Constitution*. <http://www.myajc.com/news/news/school-administrators-re-evaluate-use-of-metal-det/nWqC4/>.
256. Nilsson, F. (2009) "The Cost of a Network Video System," *Intelligent Network Video: Understanding Modern Video Surveillance Systems*, Second Edition, Boca Raton, FL: CRC Press, Inc.
257. Nyland, C., Forbes-Mewett, H., and Marginson, S. (2010) "The international student safety debate: moving beyond denial." *Higher Education Research & Development*, 29(1), 89–101.
258. Oakes, Charles, PhD. (October 2014) "The Bollard: Non-Crash and Non-Attack-Resistant Models," *Whole Building Design Guide*. <https://www.wbdg.org/resources/bollard.php>.
259. Oakes, Charles, PhD. (October 2014) "The Bollard: Crash and Attack-Resistant Models." *Whole Building Design Guide*. https://www.wbdg.org/resources/bollard_arm.php#rcas.
260. Obratzkova, M. (2014) "Security and society under examination after school shooting." Retrieved from http://rbth.com/society/2014/02/04/security_and_society_under_examination_after_school_shooting_33839.html.
261. Ochberg, F. (2012) "Why does America lead the world in school shootings?" Retrieved from <http://globalpublicsquare.blogs.cnn.com/2012/02/28/why-does-america-lead-the-world-in-school-shootings/>
262. Ohsako, T. (1997) "Violence at School: Global Issues and Interventions." *Studies in Comparative Education*. UNESCO Publishing: Paris, France.
263. Osler, A., and Starkey, H. (2006) "Education for democratic citizenship: a review of research, policy and practice 1995–2005." *Research Papers in Education*, 21(4), 433–466
264. Page-Jones, A. B. (2008) "Leadership behavior and technology activities: The relationship between principals and technology use in schools." Doctoral dissertation, University of Central Florida Orlando, Florida.
265. Pao, W. (2014) "How security enhances metro emergency management." Agmag.com. <http://www.asmag.com/showpost/17811.aspx>.
266. Pardee, G. (2014) "Russia is installing video cameras in school classrooms." Retrieved from <http://www.vice.com/read/russia-is-installing-video-cameras-in-school-classrooms>.
267. Pearce, J. (2012) "The case for open source appropriate technology." *Environment, Development and Sustainability*, 14(3), 425–431. <http://link.springer.com/article/10.1007%2Fs10668-012-9337-9>.
268. Pearson (2016) "Index: Which countries have the best schools?" Retrieved from <http://thelearningcurve.pearson.com/index/index-ranking>.

269. Pease, K. (1999) "A Review of Street Lighting Evaluations." K. Painter and N. Tilley (Eds). *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention*. Crime Prevention Studies, Vol. 10. Monsey, New York: Criminal Justice Press.
270. Perumean-Chaney, S. E., and Sutton, L. M. (2013) "Students and perceived school safety: The impact of school security measures." *American Journal of Criminal Justice*, **38**(4), 570–588.
271. Perezniето, P., Harper, C., Clench, B., and Coarasa, J. (2010) "The economic impact of school violence: A report for Plan International." *London: Plan International & Overseas Development Institute*, **2**.
272. Phaneuf, S. W. (2009) *Security in Schools: Its Effect on Students*. LFB Scholarly Publishing, LLC.
273. Phippen, Weston (26 February 2014) "Pinellas County schools to be sniffed for guns by police dogs" *Tampa Bay Times*. Retrieved 4 November 2015 from <http://www.tampabay.com/news/publicsafety/pinellas-county-schools-to-be-sniffed-for-guns-by-police-k-9s/2167612>.
274. Pittman, E. (2010) "Police Departments Connect to School District Camera Feeds to Aid Incident Response." *Education Digest: Essential Readings Condensed for Quick Review*, **76**(3), 62–64.
275. Plan International and International Center for Research on Women (2015) "Are school safe and equal places for girls and boys in Asia: Research findings on school-related gender-based violence." Retrieved from http://www.ungei.org/resources/files/SRBVAsia_ICRW_Plan.pdf.
276. Planos, J. (2 April 2015) "Do Bulletproof Whiteboards Protect Children or Traumatize Them?" *Pacific Standard*. Retrieved 4 September 2015 from <http://www.psmag.com/nature-and-technology/do-bulletproof-whiteboards-protect-children-or-traumatize-them>.
277. Poipoi, M. W. U., Agak, J. O., and Kabuka, E. K. (2011) "Perceived home factors contributing to violent behaviour among public secondary school students in western province, Kenya." *Journal of Emerging Trends in Educational Research and Policy Studies*, **2**(1), 30–40.
278. Police Executive Research Forum (9 August 2009) "The BJA/PERF Body Armor National Survey: Protecting Law Enforcement Officers. Phase II Final Report." Retrieved 17 September 2015 from http://www.policeforum.org/assets/docs/Free_Online_Documents/Police_Equipment/the%20bjaperf%20body%20armor%20national%20survey%202009.pdf.
279. Portillos, E. L., González, J. C., and Peguero, A. A. (2012) "Crime control strategies in school: Chicanas/os' perceptions and criminalization." *The Urban Review*, **44**(2), 171–188.
280. Pramuk, J. (17 November 2015) "Holiday Toy Story: Drones Expected to Take Off as Gifts." *NBC News*. Retrieved 30 November 2015 from <http://www.nbcnews.com/tech/gadgets/holiday-toy-story-drones-expected-take-gifts-n465051>.
281. Priks, M. (April 2008). "Do surveillance cameras affect unruly behavior? A close look at grandstands." CESifo Working Paper Series No. 2289. Available at SSRN:<http://ssrn.com/abstract=1126633>.

282. Purpura, P., Fennelly, L., Honey, G., and Broder, J. (2014). "Security Lighting for Schools." L. Fennelly and M. Perry (eds.). *The Handbook for School Safety and Security, Best Practices and Procedures*. New York: Elsevier.
283. Randazzo, M. R., Borum, R., Vossekuil, B., Fein, R., Modzeleski, W., and Pollack, W. (2006) "Threat assessment in schools: Empirical support and comparison with other approaches." *Handbook of school violence and school safety: From research to practice*, 147–156.
284. Ratliff, M. A. (2014) "Armed Employees and School Policy: The Issues and Perspectives of School Employees Regarding Armed Personnel in a Rural High School Setting." Doctoral dissertation, Cedarville University.
285. Redding, R. E., and Shalf, S. M. (2001) "The legal context of school violence: The effectiveness of Federal, state, and local law enforcement efforts to reduce gun violence in schools." *Law & Policy*, **23**(3), 297–343.
286. Rehm, R. S. (2002) "Creating a context of safety and achievement at school for children who are medically fragile/technology dependent." *Advances in Nursing Science*, **24**(3), 71–84.
287. Replace Inefficient MR16 Halogen Lamps with LEDs (2007). *Maxim Engineering Journal*, **61**, 10–13.
288. Richardson, D., Hoelscher, P., and Bradshaw, J. (2008) "Child well-being in Central and Eastern European countries (CEE) and the Commonwealth of Independent State (CIS)." *Child Indicators Research*, **1**(3), 211–250.
289. Richmond, M. (2013) "Education Under Attack: 2014." Global Coalition to Protect Education from Attack.
290. Robers, S., Kemp, J., and Truman, J. (2013) *Indicators of School Crime and Safety: 2012*. NCES 2013-036/NCJ 241446. National Center for Education Statistics, U.S. Department of Education, and Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice. Washington, DC.
291. Robinson, M. (2014) "A five-step approach to solving school security." Retrieved from <http://www.ifpo.org/resource-links/articles-and-reports/school-security-training/a-five-step-plan-to-solving-school-security/>.
292. Rochman, B. (2012) "School security: Why it's so hard to keep kids safe." Retrieved 24 September 2015 from <http://healthland.time.com/2012/12/18/school-security-why-its-so-hard-to-keep-kids-safe/>.
293. Rutkowski, L., Rutkowski, D., and Engel, L. (2013) "Sharp contrasts at the boundaries: school violence and educational outcomes internationally." *Comparative Education Review*, **57**(2), 232–259.
294. Ruto, S. (2009) "Sexual abuse of school age children: Evidence from Kenya." *Journal of International Cooperation in Education*, **12**(1), 177–192.

295. Ruzich, J. (2009) "Schools Add Background Checks for Visitors: Some critics express privacy concerns, but supporter say measure keeps children safe." *Chicago Tribune*. Retrieved from http://articles.chicagotribune.com/2009-12-04/news/0912020495_1_national-sex-offender-registry-checks-district-computer-systems.
296. SAMHSA BH-MITA (26 August 2008) *Concept of Operations Document*, Version 2.0.
297. Sandy Hook Advisory Commission (2015) *Final Report of the Sandy Hook Advisory Commission*.
298. Scarff, O. (31 October 2014) "Future Crimes: Scotland Yard tests 'violence prediction' software." *The Week*. <http://www.theweek.co.uk/crime/61121/future-crimes-scotland-yard-tests-violence-prediction-software>.
299. Schneider, M. (2002) *Do School Facilities Affect Academic Outcomes?*
300. Schneider, T. (2002) "Ensuring Quality School Facilities and Security Technologies." *Safe and Secure: Guides to Creating Safer Schools*. Northwest Regional Educational Laboratory, Washington, DC.
301. Schneider, T. (2007) "Ensuring Quality School Facilities and Security Technologies." *Effective Strategies for Creating Safer Schools*. The Hamilton Fish Institute on School and Community Violence and Northwest Regional Educational Laboratory, Washington DC.
302. Schneider, T. (2010) *School Security Technologies*. National Clearinghouse for Educational Facilities at the National Institute of Building Sciences, Washington, DC.
303. Schneier, B. (2007) "Light and Crime." *Schneier on Security*. Retrieved from https://www.schneier.com/blog/archives/2007/09/light_and_crime.html.
304. Schnyder, M. (8 November 2007) "Waggener students arrested after pellet guns found." Wave 3 News. Retrieved 4 November 2015 from <http://www.wave3.com/story/7331545/3-waggener-students-arrested-after-pellet-guns-found>.
305. School Improvement Network (2013) "Guns and school safety survey." Retrieved 24 September 2015 from <http://www.schoolimprovement.com/voe/guns-and-school-safety-survey-results>
306. School Security Task Force (2015) *New Jersey School Security Task Force Report and Recommendations*.
307. Schreck, C. J., and Miller, J. M. (2003) "Sources of fear of crime at school: What is the relative contribution of disorder, individual characteristics, and school security?" *Journal of School Violence*, 2(4), 57–79.
308. Secure Community Network Safe School Initiative (2014) Retrieved from <http://www.scnus.org/page.aspx?id=102715>.
309. *Security Magazine* (1 September 2015) "Man-traps: A Unique Solution." <http://www.securitymagazine.com/articles/77001-man-traps-a-unique-solution-1>.
310. Servoss, T. J., and Finn, J. D. (2014) "School Security: For Whom and With What Results?" *Leadership and Policy in Schools*, 13(1), 61–92.

311. Shamah, D. (2014) "School security a button-push away with new Israeli tech." *Times of Israel*. Retrieved from <http://www.timesofisrael.com/school-security-a-button-push-away-with-new-israeli-tech/>.
312. Sharpe, C. (3 September 2015) "Teachers Can Vie For White Boards, School Supply Funds." *The Dispatch*. Retrieved 30 October 2015 from <http://mdcoastdispatch.com/2015/09/03/teachers-can-vie-for-white-board-school-supply-funds/>.
313. Shaw, M. (2001) *Promoting Safety in Schools: International Experience and Action*
314. Shelton, A. J., Owens, E. W., and Song, H. (2009) "An examination of public school safety measures across geographic settings." *Journal of School Health*, **79**(1), 24–29.
315. SifyNews (2010) Retrieved from <http://www.sify.com/news/school-violence-costs-india-yearly-us-7-42-billion-news-international-kk0rasfjfbfsi.html>.
316. Singhal, R., and Jain, P. (2013) "Biometrics: Enhancing Security." *Asian Journal of Computer Science and Information Technology*, **1**(3).
317. Sjolseth, R. (2013) "LED Lighting: A Green Way to Improve Campus Safety." *Private University Products and News*. 24–26.
318. Skiba, R., and Knesting, K. (2001) "Zero tolerance, zero evidence: An analysis of school disciplinary practice." *New Directions for Youth Development*. **2001**(92), 17–43.
319. Skiba, R., Simmons, A. B., Peterson, R., McKelvey, J., Forde, S., and Gallini, S. (2004) "Beyond guns, drugs and gangs: The structure of student perceptions of school safety." *Journal of School Violence*, **3**(2-3), 149–171.
320. Slobogin, C. (2002) "Public privacy: camera surveillance of public places and the right to anonymity." *Mississippi Law Journal*. **72**.
321. Smarick, A. (2013) "America's rural schools and communities." Retrieved 24 September 2015 from <http://educationnext.org/americas-rural-schools-and-communities/>.
322. Smith, C. L., and Brooks, D. J. (2013) *Security Science: The Theory and Practice of Security*. Waltham, MA: Butterworth-Heinemann.
323. Smith, P. K. (Ed.) (2004) *Violence in schools: The response in Europe*. Routledge.
324. Snyder, T. D., and Dillow, S. A. (2012) *Digest of Education Statistics 2011*. National Center for Education Statistics.
325. Social Analysis and Intelligence Group (7 May 2015) "New Software, Second Sight, Could Have Prevented Violence in Ferguson and Maryland." *PRNewswire*. Retrieved from <http://www.prnewswire.com/news-releases/new-software-second-sight-could-have-predicted-violence-in-ferguson-and-maryland-300079241.html>
326. Solomon, L. (6 August 2015). "PB Tightens School, Requires Visitor ID to be Scanned: Drivers to swipe licenses before they enter schools as part of new Palm Beach County security system." *Sun Sentinel*. Retrieved from <http://www.sun-sentinel.com/local/palm-beach/fl-raptor-security-20150809-story.html>.

327. Standing Council on School Education and Early Childhood (2010) "National safe schools framework." Retrieved from <http://www.safeschoolshub.edu.au/documents/nationalsafeschoolsframework.pdf>
328. Stanley, M. S. (1996) "School Uniforms and Safety." *Education and Urban Society*, **28**(4), 424–35.
329. State of Connecticut, Department of Administrative Services (2014) *School Safety Infrastructure Standards*.
330. Stephens, R. (1998) "Checklist of characteristics of youth who have caused school-associated violent deaths." National School Safety Center, West Lake Village, CA.
331. Stone, W. E., and Spencer, D. J. (5 July 2010) "Using textbooks as ballistic shields in school emergency plans." *International Journal of Police Science and Management*. 12(4). Retrieved 4 September 2015 from http://heinonline.org/HOL/Page?handle=hein.journals/injposcim12&div=47&g_sent=1&collection=journals
332. Study Junction (2010) "Why students are beaten in India." Retrieved from <http://indiastudyplace.blogspot.com/2010/08/in-schools-of-india-almost-65-students.html>.
333. Summers, A., Vogtmann, W., and Smolen, S. (2012), *Consistent consequence severity estimation*. *Proc. Safety Prog.*, **31**. 9–16. doi: 10.1002/prs.10502
334. Swartz, K., Reyns, B. W., Henson, B., and Wilcox, P. (2011) "Fear of in-school victimization: Contextual, gendered, and developmental considerations." *Youth Violence and Juvenile Justice*, **9**(1), 59–78.
335. Swedberg, C. (2012) "The LED Inevitability." *Electrical Contractor*. <http://www.ecmag.com/volume/december-2012-lighting-special-report>.
336. Syed, D. (January 2015) "Technical and Operational Evaluation of Datacasting." National Institute of Justice Criminal Justice Research, Test, and Evaluation Center.
337. Terre des hommes (2016) "Egypt: Schools without violence." Retrieved from <http://www.tdh.ch/en/news/egypt-schools-without-violence>.
338. The Engineering Toolbox – Illuminance – Recommended Light Levels http://www.engineeringtoolbox.com/light-level-rooms-d_708.html.
339. *The Intelligencer/Wheeling New-Register* (25 July 2015) "School Door Barricades Draw Criticism in Ohio." Retrieved 4 December 2015 from <http://www.theintelligencer.net/page/content.detail/id/638399/School-Door--Barricades-Draw-Cri---.html>.
340. The Window Film Company. "Privacy Window Films." Retrieved 21 October 2015 from <http://www.windowfilm.co.uk/commercial/privacy>.
341. Theriot, M. T. (2009) "School resource officers and the criminalization of student behavior." *Journal of Criminal Justice*, **37**(3), 280–287.

342. Thomas, S., and Regnier, C. (29 November 2012) "Loaded Gun Found at High School; Police Use Dogs To Search Lockers." Retrieved 4 November 2015 from <http://fox2now.com/2012/11/29/loaded-gun-found-at-high-school-police-use-dogs-to-search-lockers/>.
343. Tillyer, M. S., Fisher, B. S., and Wilcox, P. (2011) "The effects of school crime prevention on students' violent victimization, risk perception, and fear of crime: A multilevel opportunity perspective." *Justice Quarterly*, **28**(2), 249–277.
344. Toppo, G. (2013) "Schools safe as ever despite spate of shootings, scares." Retrieved 24 September 2015 from <http://www.usatoday.com/story/news/nation/2013/11/13/school-violence-security-sandy-hook/3446023/>.
345. Total Security Solutions (22 December 2011) "True Level 4 Bullet Proof Doors." Retrieved 9 November 2015 from <http://www.tssbulletproof.com/level-4-bullet-proof-doors/>.
346. Total Security Solutions (17 January 2013) "5 Tips for Securing School Doors & Entryways with Bulletproof Materials to Increase Security." Retrieved December 2015 from <http://www.tssbulletproof.com/increase-school-security-with-bulletproof-glass/>.
347. Tyrrell, J. (8 October 2009) "Mattituck H. S. student shot while sitting in class," *Newsday*. Retrieved 9 November 2015 from <http://www.newsday.com/long-island/suffolk/mattituck-h-s-student-shot-while-sitting-in-class-1.1511027>.
348. *UAS News* (24 September 2013) "UAV: fixed wing or rotary?" Retrieved 17 November 2015 from <http://www.suasnews.com/2013/09/25214/uav-fixed-wing-or-rotary/>.
349. Underwriters Laboratories (2014) "UL 153 Standard for Portable Electric Luminaires," 54–9.
350. UNICEF (2013) "Central African Republic: Seventy per cent of school children still not in classrooms." Retrieved from http://www.unicef.org/media/media_70686.html.
351. University of Southern Mississippi, National Center for Spectator Sports Safety and Security (2015) *Interscholastic Athletics and After-School Safety and Security: Best Practices Guide*. 1st Edition.
352. UrbanPro (2015) "The importance of security in Indian schools: How Safe is your child?" Retrieved from <https://www.urbanpro.com/a/the-importance-of-security-in-indian-schools-how-safe-is-your-child>.
353. U.S. Department of Education, NCES, Fast Response Survey System (FRSS) 106 (2014) "School Safety and Discipline: 2013–14."
354. U.S. Department of Education, NCES, Schools and Staffing Survey (SASS). (2011–2012) "Public School Principal Data File" and "Private School Principal Data File."
355. U.S. Department of Education, Office of Elementary and Secondary Education, Office of Safe and Healthy Students (2013) *Guide for Developing High-Quality School Emergency Operations Plans*.
356. U.S. Department of Education, Office of Safe and Drug-Free Schools (2008) *A Guide to School Vulnerability Assessments: Key Principles for Safe Schools*, Washington, DC.

357. U.S. Department of Education, Office of Safe and Drug-Free Schools (2007) *Practical Information on Crisis Planning: A Guide for Schools and Communities*, Washington, DC.
358. U.S. Department of Education, Office of Safe and Healthy Students, Readiness and Emergency Management for Schools TA Center. Retrieved 9 December 2015 from http://rem.s.ed.gov/docs/NIMS_ComprehensiveGuidanceActivities_2009-2010.pdf.
359. U.S. Department of Energy (2015) "LED Lighting facts." <http://www.lightingfacts.com/>.
360. U.S. Department of Justice, Office of Justice Programs, NIJ (May 2014) "Comprehensive School Safety Initiative Report."
361. U.S. Department of Homeland Security (2011) *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*, Washington, DC.
362. U.S. Department of Homeland Security, FEMA (2010) *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide 101*. Version 2.0, Washington, DC.
363. U.S. Department of State (2012) "Country reports on human rights practices for 2012: Mali 2012 human rights report." Retrieved from <http://www.state.gov/documents/organization/204352.pdf>.
364. U.S. Government Accountability Office (13 November 2014) "Bureau of Indian Education Needs to Improve Oversight of School Spending." GAO-15-121. <http://www.gao.gov/products/GAO-15-121>.
365. U.S. Government Printing Office (2007) Energy Independence and Security Act of 2007. Public Law 110-140.
366. USAID (2014) "Mexico crime and violence prevention program: Quarterly Report (April–June 2014)." Retrieved from http://pdf.usaid.gov/pdf_docs/PA00K2J4.pdf.
367. Vaillancourt, T., et al. (2010) "Places to avoid: Population-based study of student reports of unsafe and high bullying areas at school." *Canadian Journal of School Psychology*, **25**(1), 40–54.
368. Valcourt, S. A., Chamberlain, K., McMahon, B., and Kun, A. (May 2007) "Systems Engineering of Datacasting for Public Safety Vehicles." Technologies for Homeland Security, 2007 IEEE Conference. Retrieved 3 September 2015 from <http://www.catlab.sr.unh.edu/Reference/Download.pm/2597/Document.PDF>.
369. Van Jaarsveld, L. (2008) "Violence in schools: a security problem?" *Acta Criminologica: CRIMSA Conference: Special Edition 2*, 175–188.
370. Villano, M. (2008) "What Are We Protecting Them From: By Mandating Schools Restrict Internet Access, CIPA and Other Federal and State Legislation Intend to Guard Student's Safety Online-But All They May Be Doing Is Keeping Vital Educational Technology out of the Classroom." *Technological Horizons in Education*, **35**(5), 48.
371. Virginia Department of Criminal Justice Services (2104) *2014 School Safety Inspection Checklist for Virginia Public Schools*.
372. Virginia Tech Review Panel (August 2007) "Mass Shootings at Virginia Tech: Report of the Review Panel." Retrieved 2 September 2015 from <https://governor.virginia.gov/media/3772/fullreport.pdf>.

373. Volokh, A., and Snell, L. (1997) "School Violence Prevention: Strategies To Keep Schools Safe." Policy Study No. 234.
374. Vossekuil, B. (2002) *The Final Report and Findings of the Safe School Initiative: Implications for the prevention of school attacks in the United States*. DIANE Publishing.
375. Vossekuil, B., Fein, R., Reddy, M., Borum, R., and Modzeleski, W. (2004) *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States*. U.S. Secret Service and U.S. DoED.
376. Vryonides, M. (2014) "Interethnic violence in schools across European countries." *Children's Voices: Studies of Interethnic Conflict and Violence in European Schools*, 49.
377. Wade, K. K., and Stafford, M. E. (2003) "Public School Uniforms' Effect on Perceptions of Gang Presence, School Climate, and Student Self-Perceptions." *Education and Urban Society*, 35(4), 399–420.
378. Wallace, K. (2014) "School system hires former FBI agent to probe social media." CNN. Retrieved from <http://www.cnn.com/2013/11/08/living/schools-of-thought-social-media-monitoring-students/>.
379. Warnick, B. R. (2007) "Surveillance cameras in schools: An ethical analysis." *Harvard Educational Review*, 77(3), 317–343.
380. Wayland, B. A. (2015) *Emergency Preparedness for Business Professionals: How to Mitigate and Respond to Attacks Against Your Organization*. Butterworth-Heinemann.
381. Whitlock, C. (26 November 2014) "Near Collisions between drones, airliners surge, new FAA reports show." *Washington Post*. Retrieved 30 November 2015 from https://www.washingtonpost.com/world/national-security/near-collisions-between-drones-airliners-surge-new-faa-reports-show/2014/11/26/9a8c1716-758c-11e4-bd1b-03009bd3e984_story.html.
382. Wikipedia (5 August 2015) "Broadcast signal intrusion." Retrieved 2 September 2015 from https://en.wikipedia.org/wiki/Broadcast_signal_intrusion.
383. Wilcox, P., May, D. C., and Roberts, S. D. (2006) "Student weapon possession and the "fear and victimization hypothesis: Unraveling the temporal order." *Justice Quarterly*, 23(4), 502–529.
384. Williams, K., and Corvo, K. (2005) "That I'll Be Killed: Pre-Service and In-Service Teachers' Greatest Fears and Beliefs about School Violence." *Journal of School Violence*, 4(1), 47–69.
385. Wilson, M. D. (3 November 2015) "Burbank High School locked down after bullet punctures occupied classroom window." *My San Antonio*. Retrieved 9 November 2015 from <http://www.mysanantonio.com/news/local/article/Burbank-High-School-locked-down-after-bullet-hits-6607607.php>.
386. Window Film Depot. "Frequently Asked Questions." Retrieved 3 December 2015 from <http://www.windowfilmdepot.com/frequently-asked-questions.html>.

387. Winske, C. (2015) "Seven solutions to secure school campuses." Retrieved from http://www.securitysales.com/article/7_solutions_to_secure_school_campuses
388. Woodford, C. (17 September 2014). "'Smart' windows (electrochromic glass)." Retrieved 3 December 2015 from <http://www.explainthatstuff.com/electrochromic-windows.html>.
389. Wren, A., and Spicer, B. (1 February 2007) "Schools, Security and Video: 6 Tips for Surveillance Deployment." Retrieved from securitysolutions.com.
390. Young, C. (2014) *The Science and Technology of Counterterrorism: Measuring Physical and Electronic Security Risk*. Butterworth-Heinemann.
391. Zablon, N. O., Areba, N. G., Monga're, E., Rael, O., and Robert, M. (2014) "Implementation of Safety Standards and Guidelines in Public Secondary Schools in Marani District, Kisii County, Kenya." *Journal of Education and Practice*, **5**(13), 111–123.
392. Zhang, A., Musu-Gillette, L., and Oudekerk, B.A. (2016). *Indicators of School Crime and Safety: 2015* (NCES 2016-079/NCJ 249758). National Center for Education Statistics, U.S. Department of Education, and Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice. Washington, DC.

This page intentionally left blank.

Appendix B. CASE STUDY QUESTIONNAIRE

CASE STUDY INTERVIEW QUESTIONS

Date of Interview: _____

Interviewers: 1) _____

2) _____

Demographics:

1. Name of Interviewee(s):
2. Position (Job Title):
3. Years of experience in this position:
4. Years of experience in school environment:
5. Years of experience dealing with school security:
6. Contact Information (email):
7. Contact Information (phone):
8. School District:
9. City, County, State
10. Informed Consent (method: verbal, note date and time)

Welcome:

Thank you for speaking with me (us) today. I am (state name) and I represent the NIJ Technology Research, Test, and Evaluation Center. As was mentioned in the earlier email, we are looking for information that will help us understand what technologies are currently being used in schools to prevent and mitigate crimes of violence to include how the technology is being used and its effectiveness, as well as how cost and regulation may affect the implementation of the security technologies.

Statement of Purpose:

We are interviewing several groups of stakeholders to include school districts, Federal agencies and professional organizations to gather information. We are interested in hearing how your school district is organized in terms of school security and how technology decisions are made at the district level. Your candid responses are very important as they will help shape future guidelines for school security technology solutions.

Informed Consent Statement (read verbatim):

Before we go further, I am required to read a statement to obtain your consent to be interviewed:

Your participation in this telephone interview is completely voluntary and there are no penalties for electing not to participate. Your responses to a set of questions will be recorded on paper or computer, but no audio recordings will be made. The discussion is expected to take about an hour. You may stop participating in the interview at any time with no penalty. If you do not wish to answer a question, you may say so and we will move on to the next question. If at any time you wish to have a comment removed from the documented interview notes, that request will be honored immediately. We are unable to provide any incentives or reimbursements for your participation in this interview. With your

permission, we will acknowledge your participation by name in any publications resulting from this effort. Information collected during your interview will be included in resulting documents so that other interested people may learn about school security. However, nothing that you discuss during the interview will be attributed to you by name or shared with anyone outside the project team. If you have any questions, you may ask them at any time before, during or after the interview. If you wish to ask questions later, you may contact our principal investigator, Mr. Steven Taylor, whose contact information will be provided in a follow-up email.

1. Do you have any questions regarding what I have just read to you? Y / N
2. Do you consent to be interviewed? Y / N
3. Can someone from the research team contact you at a later date to clarify your responses if needed? Y / N
4. Can we acknowledge your participation by name, title/position, and organization in documents resulting from this effort? Y / N

District-Level Budgets and Security Planning

1. Please estimate the total student enrollment of your district (K-12):
2. Please estimate the total dollars spent per student, per year:
3. Please estimate the total dollars spent on school security per student, per year:
4. Does your district have a Security Plan?
5. Is technology integrated into the plan?
6. Does your district conduct drills with students and staff? What kinds? How often?
7. Do you use any sort of metrics to evaluate effectiveness of drills?
8. How is your district's safety funded and staffed?
9. How secure is the funding for school safety? (quarterly, yearly, biennial budget, etc.)
10. How did your district select the technologies that have been implemented?
11. Are there areas of your schools which require special consideration to mitigate the possibility of school violence? (classrooms, multi-purpose rooms, library, cafeteria, gym, hallways/common areas/locker areas, entrances, parking lot, playgrounds/athletic fields, school buses)
12. Are there professional organizations or state agencies that you regularly interact with? Describe how impactful those relationships are.

Detailed Technology Utilization

School Safety Technology	In Use	Comments
Access Control – Physical Barriers		
Standard door locks (lock and key); deadbolt		
Standard window locks (latches)		
Combination locks		
Padlocks		
Electronic locks (remotely operated)		
Perimeter fencing		
Security or safety personnel		
Guarded entry gates		
Anti-ram vehicle barriers		

School Safety Technology	In Use	Comments
Bullet-resistant glass; window films		
One-way doors		
Turnstiles		
Lockdown systems		
Mantraps		
Access Control – Means of Identification		
Swipe cards (magnetic or RFID)		
Temporary ID or visitor badges		
Staff ID cards		
Student ID cards		
Access Control – Biometric Readers		
Fingerprint or handprint scanners and readers		
Iris scanners and readers		
Voice recognition		
Facial recognition		
Alarms and Sensors – Intrusion and Access Alarms		
PIR motion sensors		
Photo and laser sensors		
Open door or window sensors		
Millimeter wave motion sensors		
Tamper alarms		
Alarms and Sensors – Distress Alarms		
Distress and duress alarms or panic buttons		
Emergency call boxes		
Alarms and Sensors – Special and Environmental Alarms		
Radiological or nuclear		
Chemical or biological		
Communications – Two-way Communications		
Handheld and vehicle-mounted radios or base stations		
Police scanners		
Cellular telephones (including text messaging)		
Landline telephones		
Intercoms or PA system		
Communications – One-way Communications		
Emergency notification system		
Mass telephone communication system		

School Safety Technology	In Use	Comments
Instant mass messaging system (text)		
Automated email system		
Bullhorns		
Digital signs or billboards		
Datacasting system		
Lighting		
Indoor lights		
Outdoor lights		
Stadium lights		
Software		
Tip line		
Risk assessment or management software		
Situational awareness software		
Security planning software		
Violence prediction software		
PSIM system		
Visitor database check software		
Health or mental health information sharing software		
Social media monitoring application		
Text monitoring application		
Surveillance		
Standard video cameras		
IR cameras		
Body-worn cameras		
Smart camera or video analytics		
Gunshot location system		
GPS personnel tracking		
GPS vehicle tracking		
Weapons Detection		
Walk-through metal detectors		
Handheld (wand) metal detectors		
Radar or millimeter wave weapons detection systems		
X-ray scanner		
Other Technology Systems		
Bullet-proof white boards		
Pepper spray dispensers		
Canines		

School Safety Technology	In Use	Comments
Safes		
Drones		
Cyber and Computer Systems		
Computer systems protection		
Emails (automated email services or messaging)		
Anti-virus software		
Encryption software		

Implementation and Vulnerability Aspects of Technology

How have the technologies been impacted by the following implementation & vulnerability aspects?

Implementation Aspect	Comments
Acquisition	
Installation	
Training	
Maintenance	
Consumables	
Power requirements	
Unexpected benefits	
Limitations	
Policies	
Liabilities	
Personnel and culture of security	
Vulnerabilities	
Overcoming	
Failure modes	
Adaptive behaviors	
Consequence of failure	

Effectiveness

1. How effective you think this technology is at *preventing* acts of criminal violence from occurring in your school, *mitigating* such acts if they occur at your school, or *investigating* such acts that have occurred at your school, depending on the purpose of the technology.
2. Were other approaches or technologies considered to meet the same need?
3. Please describe how your school environment combines school safety technologies. (Schools often use technologies in combinations as part of their school safety plans. For examples, some schools may use a metal detector for students along with an x-ray machine for their bags.)

4. Have there been any significant changes in the safety technologies used in your environment in the past two years or so? What? What impact did these changes have on student behavior?
5. What one school safety technology could your district discontinue without significantly decreasing its security? Why?

Appendix C. ACRONYMS

AC	Alternating Current
AED	Automated External Defibrillator
ALICE	Alert, Lockdown, Inform, Counter, and Evacuate
AMS	Access Management System
ANSI	American National Standards Institute
ASIS	American Society for Industrial Security
ASTM	American Society for Testing and Materials
BHMA	Builders Hardware Manufacturers Association
BH-MITA	Behavioral Health Medicaid Information Technology Architecture
BIE	Bureau of Indian Education
BS	British Standard
CBRN	Chemical, Biological, and Radiological/Nuclear
CCTV	Closed-Circuit Television
CERT	Citizen's Emergency Response Team
CFL	Compact Fluorescent Lamp
CIPA	Children's Internet Protection Act
CPTED	Crime Prevention Through Environmental Design
CRI	Color Rendering Index
DC	Direct Current
DHS	Department of Homeland Security
DIN	Deutsche Institut für Normung
DoED	Department of Education
DOJ	Department of Justice
DVR	Digital Video Recorder
EMT	Emergency Medical Technician
EOP	Emergency Operations Plan
ETD	Explosive Trace Detection
fc	Foot-Candle
FEMA	Federal Emergency Management Agency
FOV	Field of View
FRSS	Fast Response Survey System
GIS	Geographic Information System
GPS	Global Positioning System

HID	High-Intensity Discharge
HIPAA	Health Insurance Portability and Accountability Act
HPS	High-Pressure Sodium
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Incident Command System
ID	Identification
IESNA	Illuminating Engineering Society of North America
IMS	Ion Mobility Spectrometry
IP	Internet Protocol
IPVM	Internet Protocol Video Market
IR	Infrared
IT	Information Technology
LEA	Local Educational Agency
LED	Light-Emitting Diode
LPS	Low-Pressure Sodium
MMW	Millimeter Wave
MOU	Memorandum of Understanding
MV	Mercury Vapor
N/A	Not Applicable
NASBE	National Association of State Boards of Education
NCEF	National Clearinghouse for Educational Facilities
NCES	National Center for Education Statistics
NIJ	National Institute of Justice
NIMS	National Incident Management System
NIOSH	National Institute for Occupational Safety and Health
NSOPW	National Sex Offender Public Website
NSSC	National School Safety Center
NVR	Network Video Recorder
ONVIF	Open Network Video Interface Forum
OSAT	Open Source Appropriate Technology
OSHA	Occupational Safety and Health Administration
PA	Public Address
PET	Polyethylene Terephthalate
PIN	Personal Identification Number
PIR	Passive Infrared

Pre-K	Pre-Kindergarten
PSIM	Physical Security Information Management
PTA	Parent Teacher Association
RDR	Remote Delay Relay
RFID	Radio Frequency Identification
RT&E	Research, Test, and Evaluation
SaaS	Software-as-a-Service
SAMHSA	Substance Abuse and Mental Health Services Agency
SASS	Schools and Staffing Survey
SMS	Short Message Service
SRO	School Resource Officer
SWAT	Special Weapons and Tactics
TSA	Transportation Security Administration
TxSSC	Texas School Safety Center
UHF	Ultra-High Frequency
UL	Underwriters Laboratories
VAC	Volts Alternating Current
VAS3	Virtual Alabama School Safety System
VDC	Volts Direct Current
VMS	Video Management System
VoIP	Voice-over Internet Protocol
WiFi	Wireless Fidelity

This page intentionally left blank.