



## Special Report: Counterterrorism

### Response 9.11

**O**n September 11, 2001, at 8:46 a.m., American Airlines flight 11, hijacked by terrorists out of Boston's Logan International Airport, crashed into the North Tower of New York City's World Trade Center (WTC). Sixteen minutes later, onlookers and television crews watched as terrorists crashed a second plane, United Airlines flight 175, also out of Boston, into the middle of the WTC's South Tower. Police officers, firefighters, rescue workers, and thousands of others trying to evacuate the burning buildings were trapped when the 110-story South Tower suddenly collapsed at 9:59 a.m. At 10:28 a.m., the 110-story North Tower also collapsed, burying and eventually destroying five other buildings and the nine below-ground levels of the WTC complex. Almost 3,000 people, including rescue workers, were killed.

According to engineers interviewed by the media, each tower was built around a central steel core surrounded by open office space. Supporting 18-inch steel tubes ran vertically along the outside of the buildings. When the planes damaged the central cores, the weight of the buildings was redistributed to the outer steel tubes, which buckled under the added weight and the intense heat of the fires. The resulting debris pile was five stories high.

As the attacks unfolded in New York City, terrorists hijacked another plane out of Dulles International Airport in northern Virginia, near Washington, D.C. At 9:40 a.m., this plane, American Airlines flight 77, crashed into the west side of the Pentagon. Shortly thereafter, reports of another hijacking began to filter in. At 10:10 a.m., United Airlines flight 93 out of Newark International Airport in New Jersey crashed in Stonycreek Township in rural Somerset County, Pennsylvania, killing all aboard. Experts believe the plane was heading for another high-visibility target, possibly the U.S. Capitol or the White House.

Immediately following the terrorist acts of September 11, the New York State Emergency Management Office asked the National Institute of Justice (NIJ) to provide onsite technology assistance. Within 24 hours, staff at NIJ's Office of Science and Technology had established

a technology support office adjacent to the WTC complex to help coordinate technology assistance activities with search and rescue officials. Two technical representatives from NIJ staffed the technology support office during the initial search, rescue, and recovery operations.

"We were asked onsite for two reasons," says Chris Tillery, Senior Program Manager of NIJ's Critical Incident Technology Program and one of the first technical representatives at the WTC. "We were there to help identify the technology requirements of the Federal Emergency Management Agency's Urban Search and Rescue (US&R) teams and the New York City Fire Department (FDNY), and to work with them in developing solutions."

"Because of the enormity of the task that lay before search and rescue personnel, it was essential that all of our resources came into play. Through NIJ's National Law Enforcement and Corrections Technology Center [NLECTC] system and its technical partners, our onsite technical support team was able to leverage technical resources, equipment, and expertise to deliver technology that was rugged and dependable enough to assist the search and rescue teams and fire department."

The first team to arrive in support of the technical support office was from the NIJ-funded Savannah River Technology Center (SRTC) at the U.S. Department of Energy's (DOE's) Savannah River Site near Aiken, South Carolina. The team consisted of electrical and mechanical engineers, a chemist, and a technician. They brought more than \$500,000 worth of equipment that included cameras, microphones, crawlers, boroscopes, and other tools that could reach into inaccessible and hazardous spaces in the voids under the rubble. The SRTC team and NIJ staff provided onsite technology expertise and made real-time engineering modifications and repairs to equipment to fit specific US&R needs as they arose. To aid FDNY in detecting, documenting, and recording victims trapped and human remains found during cleanup, NIJ set up a perimeter surveillance system and trained firefighters in its use.

The next teams to arrive to help the technical support office were from the Center for Civil Force Protection, which is funded by NIJ and located at DOE's Sandia National Laboratories (SNL) near Albuquerque, New Mexico; and from Pennsylvania State University's (PSU's) Applied Research Laboratory. SNL engineers had developed surveillance systems for search dogs that allow their handlers to see what the dogs see in areas where humans cannot go. The representatives from PSU provided expertise in advance acoustic technologies and terrain assessment.

Offsite, NLECTC–Southeast in Charleston, South Carolina, coordinated the identification, collection, and delivery of more than \$850,000 worth of equipment made available through its 1033 Program. In addition, staff from NIJ's Investigative and Forensic Sciences Division and the NLECTC system began identifying forensic and investigative assistance resources. The Federal Laboratory Consortium (FLC) for Technology Transfer also helped identify technologies that could aid in the WTC search, rescue, and recovery mission. The FLC rapidly disseminated information to more than 700 Federal laboratories and centers. Numerous facilities offered to help with technology and expertise.

“The operational challenges and hazardous working conditions faced by the urban search and rescue teams limited the practical use of many technologies,” according to Joe Cecconi, an NIJ Program Manager with an engineering background who also went to the WTC site. “However, groundwork was established for future partnerships.” He says that since the WTC attack, NIJ has continued to provide technology information, assistance, and expertise to the public safety community in the areas of critical incident planning and response.

“As a result of the events of September 11, we have received many valuable recommendations from the responding agencies and departments in terms of new technology research and development and in modifying existing technologies.”

## Search and Rescue Assistance

**Canine Camera.** On September 20 at the WTC site, the Florida US&R team used the first of six canine cameras. The cameras provided views of remote areas that dogs could access but humans could not. SNL developed these canine cameras and modified them onsite. Lighting was added so the dogs could search in dark areas. In addition, an audio control allowed handlers to give commands to their dogs. The California US&R team also deployed the canine cameras.

**Pole Camera.** The NIJ team fabricated a pole camera to replace one that had been broken during an earlier search and rescue effort. During a debriefing, the team recommended changes to enhance the pole camera's

design and performance and advised that commercial versions are also available.

**Void-Search or Drop Camera.** Search and rescue teams used the void-search or drop camera to explore several voids in the rubble, stairwells, and an underground parking lot. The Pennsylvania and Texas US&R teams used a makeshift drop camera assembled from commercial technology primarily intended for deployment-tethered mobile robots. SRTC engineers converted an underwater pan/tilt/zoom/lights camera assembly into a portable unit for vertical deployment into 100-foot voids. Although the temperatures in some of these voids were estimated to be 1,000 degrees Fahrenheit, the camera performance was unaffected.

**Perimeter Surveillance.** At the request of FDNY, NIJ staff developed a system of cameras for perimeter surveillance of the WTC site. With technical and manpower assistance from the Nassau County (New York) Police Department, NIJ staff and SRTC engineers set up six strategically placed cameras that allowed searchers to remotely monitor sites, identify areas with potential victims, and send in appropriate response teams.

**Thermal Imaging.** NIJ made available thermal imagers and trained US&R teams in their use. Thermal imagers “see” what are essentially differences in temperature—differences as small as 1 degree. They can show the location of anything that retains heat, such as a living person.

## Communications and Interoperability Assistance

**ACU-1000.** NIJ's AGILE program is evaluating an ACU-1000 communications switch at the Alexandria, Virginia, Police Department. This switch provides communications interoperability during critical incidents by linking voice communications among disparate radio systems, thereby enabling different agencies and jurisdictions to communicate with each other. Following the September 11 attack on the Pentagon, the ACU-1000 was activated and partner agencies were advised that the ACU-1000 was available. (Partner agencies include the FBI, the Secret Service, and the U.S. Park, U.S. Capitol, Metropolitan D.C., Metro Transit, Maryland State, Virginia State, Arlington, and Alexandria Police Departments.) A number of active channels were monitored, which enabled ACU-1000 testbed personnel to provide dispatchers with information from other departments; direct radio links between the partner agencies were not requested. The testbed personnel provided communication support throughout the response to the Pentagon attack and remained ready to provide direct radio links between the responding agencies. They also completed the FBI's request to program a new frequency in the ACU-1000 for their Washington field office communications.

**Mobile and Voice Data Communications.** The New York State Emergency Management Office requested communications assistance from NLECTC–Northeast employees who work for the New York State Technology Enterprise Corporation (NYSTEC), a technology adviser to the New York State government. By 10 a.m. on September 11, NYSTEC had mobilized a state-of-the-art mobile and voice data communications center to help the State quickly set up military communications throughout New York City and to reestablish the critical data lines that connect Albany to numerous State facilities in the city.

## Excess Property and Equipment Assistance

**1033 Program.** NLECTC–Southeast coordinated a systemwide effort to send excess boots, clothing, protective and work gloves, ropes, gas masks, ballistic-resistant helmets, laptop computers, and other needed equipment to rescuers. The equipment was secured through the Georgia 1033 Coordinator’s Office and the U.S. Department of Defense’s Defense Reutilization Marketing Office in Fort Jackson, South Carolina. The Charleston (South Carolina) Police Department and other law enforcement agencies provided a police escort for the trucks that transported the equipment.

**Refrigerated Storage.** In response to a request from the New York State Police, NLECTC identified and arranged the delivery of two walk-in portable and four semi-tractor mobile refrigerated units for storage of DNA samples from the WTC site at the New York State Police Forensic Investigation Center.

## Investigative and Forensic Assistance

**Audio Technologies.** At the request of the New York County (Manhattan) District Attorney’s Office, NLECTC–Northeast’s Law Enforcement Analysis Facility (LEAF) staff prepared numerous audio technologies for possible use. These included a speaker identification program that can identify a person from as little as one word of speech and a speech enhancement program that can remove noise or interference from a variety of media without distorting the words. LEAF staff processed an audiotape that contained Arabic using the Air Force Research Laboratory’s speech enhancement technologies. Once the processing was completed, the tape was returned to the District Attorney’s Office for further investigation.

**DNA Analysis.** NIJ offered hardware and software assistance to the Armed Forces DNA Identification Laboratory and the New York City and State crime laboratories. These labs are using forensic DNA testing to identify victims of the September 11 attacks.

NIJ further empaneled the Kinship and Data Analysis Panel of renown experts in the areas of parentage testing,

genetics, genomics, information technologies, bionformatics, and others. This panel has been actively involved in recommending and developing protocols, methodologies, and analytical support for the mass identification project being undertaken at the WTC site.

## Other Assistance

**New York Electronic Crimes Task Force.** The U.S. Secret Service New York field office and the New York Electronic Crimes Task Force (NYECTF) office were in Building 7 of the WTC, which was destroyed. Fortunately, the entire staff survived, but all records, computers, and software tools were lost. NLECTC–Northeast, which has worked with NYECTF on projects that include the Computer Forensic Experiment 2000 and the International Conference on Electronic Crime, helped NYECTF to recover their operational capability. NLECTC–Northeast assisted NYECTF in acquiring new computers, software, and such office equipment as fax machines and safes.

**Odor Perception Inhibitor.** The Office of Law Enforcement Technology Commercialization (OLETC) in Wheeling, West Virginia, arranged for thousands of vendor-donated odor perception inhibitor packets for search and rescue workers. Putrex (formerly known as Carry-On) is a gel-based inhibitor that isolates and eliminates putrescine and cadaverine, two compounds associated with the odor of decomposing or burnt flesh. The product, however, does not inhibit other odors, such as natural gas, that could signal an environmental hazard. OLETC had assisted in the commercialization of this product in early 2001.

## Critical Incident Technology Program: Built on Partnerships

*No matter what the critical incident, first responders face similar problems: less than total response coordination across jurisdictions and among agencies, lack of training, and equipment deficiencies.*

*No matter what the critical incident, efficient and effective response requires partnerships—partnerships among agencies at critical incident sites as well as partnerships for providing training, developing new technologies, and exploring ways to prevent terrorist and other criminal acts.*

*No matter what the critical incident, without a unified, coordinated response that uses advanced equipment and technologies, lives will be lost, time will be wasted, and resources will be underutilized.*

In 1997, the National Institute of Justice (NIJ), through its Office of Science and Technology (OS&T), initiated a critical incident technology program to develop solutions relating to agency coordination, personnel training, and equipment and technology development. This program

is a collaborative effort among Federal, State, and local public safety agencies.

This multidisciplinary, multiagency approach extends NIJ's objective of preparing law enforcement and public safety communities to respond to terrorist incidents by building on existing capabilities for handling other emergencies.

"What is important to understand about NIJ's critical incident technology program is that we don't just look at the needs of law enforcement, we focus on problems common to all public safety agencies," says Chris Tillery, the Senior Program Manager for NIJ's Critical Incident Technology Program.

"Coordinating a combined response among agencies from multiple jurisdictions is difficult during any critical incident, whether it's a terrorist attack, a natural disaster, or an industrial accident. But through these partnerships, NIJ identifies gaps in existing technology efforts and leverages its \$10 million annual investment with investments from other agencies that total hundreds of millions of dollars. Since its inception in 1997, this collaborative effort has already produced a number of new technologies. Some already are in use, and some are still in the testing stage."

## Biohazard and Chemical Defense

- The Office of Law Enforcement Standards (OLES) at the National Institute of Standards and Technology coordinates the development of standards for chemical and biological protective equipment for responders. OLES, which is funded by NIJ, collaborates with the Technical Support Working Group (TSWG), a joint effort of the Departments of Defense, State, Justice, and Energy; the FBI's National Domestic Preparedness Office; the National Fire Protection Association, a nonprofit organization; the Centers for Disease Control and Prevention's National Institute for Occupational Safety and Health; and the Office of Justice Programs' Office for Domestic Preparedness, among others. In June 2000, OLES produced the first in a series of guides relating to biohazard and chemical defense. The remaining guides were placed on the Internet, in draft, in October 2001 in response to the events of September 11.
- TSWG and the FBI are collaborating with NIJ on an assessment of potential chemical and biological threats. This study includes both a historical analysis of chemical and biological incidents and a scientific assessment of the physical properties of chemical and biological agents to determine the true threat they pose. Sandia National Laboratories (SNL) also is developing a model to assess the vulnerability of the country's chemical production infrastructure.
- The Whitehead Institute for Biomedical Research and Nanogen, Inc., have received NIJ funding to develop

portable forensic DNA analysis devices. These units would be able to type and subtype bacterial strains quickly, thus allowing for rapid and accurate medical treatment and possible identification of the origins of a biohazard substance.

- Through the Joint (Justice-Defense) Program Steering Group (JPSG), NIJ, Argonne National Laboratory, SNL, and the Washington (D.C.) Metropolitan Area Transit Authority are developing a prototype real-time early warning chemical detection and emergency alarm system for subways.
- In cooperation with TSWG, NIJ is sponsoring the development of a low-cost device that would warn wearers about exposure to biological and chemical hazards. The monitor would alert users in enough time to allow them to put on an escape mask. Prototype evaluations, including an assessment by the U.S. Army Soldier and Biological Chemical Command, currently are under way.
- Through JPSG, NIJ is working with TSWG to develop a protective mask that would give first responders time to exit a hazardous area, alert the proper officials, and stop others from entering the area. The mask, which is intended for use in situations where authorities receive little or no warning, needs to be lightweight, easily carried and used, and inexpensive. It also could be used to protect victims during evacuation.

## Communications and Interoperability

- NIJ's AGILE program addresses communications interoperability and information sharing issues that result when agencies from multiple jurisdictions respond to a critical incident. Both short-term and long-term interoperability solutions are being developed for wireless telecommunications and information sharing technology based on three major program elements: (1) standards; (2) research, development, test, and evaluation; and (3) outreach. Through this approach, AGILE aims to raise the awareness of interoperability issues and disseminate short-term solutions, lessons learned, and best practices so that policymakers and public safety leaders can make informed, cost-effective decisions.
- INFOTECH uses existing systems and networks to promote information sharing among law enforcement agencies. It is fully operational in two Florida county sheriffs' offices and is in the implementation stages in California, Oregon, and Virginia. The system, created in cooperation with the U.S. Navy Space and Naval Warfare Systems Center (SPAWAR) in Charleston, South Carolina, expands on technology originally developed by the U.S. Department of Defense's Defense Advanced Research Projects Agency.
- NIJ is in the initial stages of implementing a testbed to identify technology gaps and evaluate commercially available critical incident management software. The

testbed is being developed in collaboration with Camber Associates, the District of Columbia's Emergency Management Agency, the Institute for Security Technology Studies at Dartmouth College, and SPAWAR-Charleston.

## Explosives Detection and Remediation

- Operation America is an advanced training opportunity for bomb technicians. This event features examples of the latest techniques that a bomber could use to construct a complex, hard-to-defeat device. Techniques include advanced initiation sequences, antidefeat mechanisms, and booby traps. Personnel from SNL demonstrate the latest technology and approaches to render safe such advanced devices.
- An interactive training CD-ROM has been developed for bomb technicians. This individual instruction serves as refresher training for the basic bomb technician course taught at the FBI's Hazardous Devices School (HDS). The CD is currently under review by HDS.
- Bomb squads can obtain a virtual library of information previously published by the FBI in three bulletin series: Bomb Technician, Investigator, and General Information. Three CDs provide instant access to information that could prove valuable during a bomb response call or an investigation. The CDs are available from the FBI Bomb Data Center.
- Recommendations from prototype testing by the Kansas-Missouri Bomb Technician Working Group are being incorporated into the design of a small, portable, inexpensive device that could safely disable large fuel-fertilizer bombs such as the one that destroyed the Murrah Federal Building in Oklahoma City. The Naval Surface Warfare Center's Indian Head Division is developing the technology.
- NIJ, through TSWG, conducted a study to identify practitioner requirements for bomb robots. A solicitation for development of a robot that would meet these requirements was released in 2001.

## Security

- NIJ, the Federal Aviation Administration's (FAA's) Aviation Security Research and Development Division, and a focus group within the Biometrics for Improving Aviation Security Working Group are addressing concerns about the use of biometrics to improve civil aviation security. Face-recognition technology, which compares a person's face with images stored in a database, is of particular interest. This technology could verify access for airline crew and airport personnel. It also could identify individuals who are on a watch list. This technology could possibly be integrated with weapons

detection portals to improve screening of passengers and employees.

- A portable system developed by Raytheon Company uses low-power radar to locate and track multiple individuals through walls. The system, which is a modification of a commercial motion detector, can distinguish people through concrete or brick walls up to 8 inches thick at a range of more than 75 feet. A prototype should be ready for evaluation in Fiscal Year 2002. The Air Force Research Laboratory also is participating in the project.

## Weapons Detection

- With funding from NIJ, the U.S. Department of Energy's Idaho Environmental and Engineering Laboratory has developed a walk-through weapons detection portal that detects anomalies in the Earth's magnetic field caused by ferro-magnetic material commonly found in weapons. This device does not pick up ordinary objects such as jewelry and keys, which allows many people to be scanned rapidly. It presently is in use in the Bannock County, Idaho, courthouse and in a New York City high school. The FAA has a portal under evaluation. The portal was commercialized in 2000 by Quantum Magnetics and Milestone Technologies as the SecureScan 2000.
- Through a grant from NIJ, Trex Enterprises has demonstrated a portable system to detect concealed weapons in crowds. The device uses a passive millimeter wave imager to pick up differences in heat energy between a person's body and objects the person is carrying. These objects appear as distinct images on a real-time video. NIJ is working with the FAA to explore the possibility of placing this technology, along with the weapons detection portal, into the Nation's airports.

## Other Initiatives

- The NIJ-funded Center for Civil Force Protection offers assistance to State and local law enforcement agencies and other public safety agencies on combating terrorism and responding to other critical incidents. Information and assistance are available in such areas as architectural safety, biometrics, bomb suits, and vulnerability analyses.

Other NIJ partners in the Critical Incident Technology Program include the Centers for Disease Control and Prevention, Eastern Kentucky University, the InterAgency Board for Equipment Standardization and InterOperability, the Oklahoma City National Memorial Institute for the Prevention of Terrorism, and the OJP Office for Domestic Preparedness.

*For additional information, visit the NLECTC Virtual Library page on JUSTNET at [www.justnet.org](http://www.justnet.org).*

## If You Need More Information

The following list can assist public safety personnel in finding information and training resources in their efforts to prevent terrorist attacks and respond to them should they occur.

### Chemical/Biological Defense

#### Publications

*Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders.* NIJ Guide 100–00. June 2000. Volume I, NCJ 184449. Volume II, NCJ 184450.\*

*HotZone '99: Advanced Technology Needs for Consequence Management of Biological Terrorism.* 1999. NCJ 180809.\*

*Guide for the Selection of Chemical and Biological Decontamination Equipment for Emergency First Responders.* NIJ Guide 103–00. October 2001.\*

*Guide for the Selection of Communication Equipment for Emergency First Responders.* NIJ Guide 104–00. Available soon.\*

*Guide for the Selection of Personal Protective Equipment for Emergency First Responders.* NIJ Guide 102–00. Available soon.\*

*An Introduction to Biological Agent Detection Equipment for Emergency First Responders.* NIJ Guide 101–00. Available soon.\*

#### Websites

Center for Civilian Biodefense Strategies, Johns Hopkins University: [www.hopkins-biodefense.org](http://www.hopkins-biodefense.org).

Chem-Bio.com: [www.chem-bio.com](http://www.chem-bio.com)

National Institute for Occupational Safety and Health, Centers for Disease Control and Prevention: [www.cdc.gov/niosh/homepage.html](http://www.cdc.gov/niosh/homepage.html)

### Cybercrime

#### Publications

*Electronic Crime Scene Investigation: A Guide for First Responders.* NIJ Guide. July 2001. NCJ 187736.\*

*Electronic Crime Needs Assessment for State and Local Law Enforcement.* NIJ Research Report. March 2001. NCJ 186276.\*

*Best Practices for Seizing Electronic Evidence.* A joint project of the International Association of Chiefs of Police and the U.S. Secret Service. 2000.\*\*

*State and Local Law Enforcement Needs to Combat Electronic Crime.* NIJ Research in Brief. August 2000. NCJ 183451.\*

*Needs and Prospects for Crime-Fighting Technology: The Federal Role in Assisting State and Local Law Enforcement.* By William Schwabe. Prepared for the White House Office of Science and Technology Policy by RAND. Publication MR–1101–OSTP. 1999. NCJ 185312.\*

#### Websites

Computer Crime and Intellectual Property Section, U.S. Department of Justice: [www.cybercrime.gov](http://www.cybercrime.gov)

Department of Defense Computer Forensics Laboratory: [www.dcfll.gov](http://www.dcfll.gov)

Internet Fraud Complaint Center, Federal Bureau of Investigation and National White Collar Crime Center: [www.ifccfbi.gov](http://www.ifccfbi.gov)

National Center for Forensic Science: [ncfs.ucf.edu](http://ncfs.ucf.edu)

National Cybercrime Training Partnership: [www.nctp.org](http://www.nctp.org)

National Law Enforcement CyberScience Laboratory–Northeast: [www.justnet.org/nlectcne](http://www.justnet.org/nlectcne)

National White Collar Crime Center: [www.nw3c.org](http://www.nw3c.org); [www.cybercrime.org](http://www.cybercrime.org)

### Explosives Detection and Remediation

#### Publications

*Technology Development, Implementation, and Evaluation for Collection and Analysis of Explosives Trace Chemical Evidence.* August 2000. NCJ 189913.\*

*A Guide for Explosion and Bombing Scene Investigation.* NIJ Research Report. June 2000. NCJ 181869.\*

*Guide for the Selection of Commercial Explosives Detection Systems for Law Enforcement Applications.* NIJ Guide 100–99. September 1999. NCJ 178913.\*

*Survey of Commercially Available Explosives Detection Technologies and Equipment.* September 1998. NCJ 171133.\*\*

#### CDs

Bomb Disposal and Investigation Resources: three CDs contain 30 years of three FBI bulletin series: *Bomb Technician, Investigator, and General Information*. To order, contact the FBI Bomb Data Center, 935 Pennsylvania Avenue, Washington, DC 20535; 202–324–2696.

#### Videos

*Surviving the Secondary Device—The Rules Have Changed.* Office for Domestic Preparedness. 1997. NCJ 168105.\*

## Websites

Arson & Explosives National Repository, Bureau of Alcohol, Tobacco and Firearms: [www.atf.treas.gov/axis2/index.htm](http://www.atf.treas.gov/axis2/index.htm)

Federal Bureau of Investigation Bomb Data Center: [www.fbi.gov](http://www.fbi.gov)

## Infrastructure/Physical Security

### Publications

*Guide to the Technologies of Concealed Weapon and Contraband Imaging and Detection.* NIJ Guide 602–00. February 2001. NCJ 184432.\*

*User's Guide for Hand-Held and Walk-Through Metal Detectors.* NIJ Guide 600–00. January 2001. NCJ 184433.\*

*Hand-Held Metal Detectors for Use in Concealed Weapon and Contraband Detection.* NIJ Standard–0602.01. September 2000. NCJ 183470.\*

*Walk-Through Metal Detectors for Use in Concealed Weapon and Contraband Detection.* NIJ Standard–0601.01. September 2000. NCJ 183471.\*

*Video Surveillance Equipment Selection and Application Guide.* NIJ Guide 201–99. October 1999. NCJ 179545.\*

*Perimeter Security Sensor Technologies Handbook,* 1997. 1997.\*\*

*Hands-Off Frisking: High-Tech Concealed Weapons Detection.* June 1996.\*\*

### Videos

*Land Transportation Security Technology—An Improved Response for a Changing Threat.* 1999.\*\*

### Websites

National Infrastructure Protection Center: [www.nipc.gov](http://www.nipc.gov)  
U.S. Department of Energy: [www.energy.gov](http://www.energy.gov)

## Interoperability

### Publications

*Understanding Wireless Communications in Public Safety: A Guidebook to Technology, Issues, Planning, and Management.* March 2000, revised August 2000. NCJ 180211.\*\*

*State and Local Law Enforcement Wireless Communications and Interoperability: A Quantitative Analysis.* NIJ Research Report. January 1998. NCJ 168961.\*

*Wireless Communications and Interoperability Among State and Local Law Enforcement Agencies.* NIJ Research in Brief. January 1998. NCJ 168945.\*

## Videos

*“Why Can't We Talk?” When Lives Are at Stake.* 1998. Fact sheet, July 2000.\*\*

### Websites

NIJ's AGILE Program: [www.agileprogram.org](http://www.agileprogram.org)

Federal Communications Commission: [www.fcc.gov](http://www.fcc.gov)

National Telecommunications and Information Administration, U.S. Department of Commerce: [www.ntia.doc.gov](http://www.ntia.doc.gov)

## General Resources

### Publications

1033 Program—Excess Defense Personal Property: <http://www.dla.mil/j-3/leso/section1033.htm>; and 1122 Program—State and Local Law Enforcement Equipment Procurement Program, <http://www.dla.mil/j-3/leso/section1122.htm>. See *Federal Property and Equipment Manual: Federal Sources of Personal Property for Law Enforcement.* Revised 2001. NCJ 172872.\*\*

*A Resource Guide to Law Enforcement, Corrections, and Forensic Technologies.* May 2001. NCJ 186822.\*

*Inventory of State and Local Law Enforcement Technology Needs To Combat Terrorism.* NIJ Research in Brief. January 1999. NCJ 173384.\*

*State and Local Law Enforcement Technology Needs To Combat Terrorism, Volume I: Inventory of Needs.* 1998. NCJ 176988.\*

*Domestic Terrorism: A National Assessment of State and Local Preparedness.* 1995. Research Report, NCJ 154149, Survey, NCJ 158329.\*

### Videos

*Surviving Weapons of Mass Destruction.* Office for Domestic Preparedness. 1999. NCJ 181435.\*

*Weapons of Mass Destruction—The First Responder.* Office for Domestic Preparedness. 1999. NCJ 181436.\*

### Websites for Federal Government Institutes, Organizations, and Programs

Bureau of Alcohol, Tobacco and Firearms: [www.atf.treas.gov](http://www.atf.treas.gov)

Centers for Disease Control and Prevention: [www.cdc.gov](http://www.cdc.gov)

–Public Health Emergency Preparedness & Response: [www.bt.cdc.gov](http://www.bt.cdc.gov)

Federal Bureau of Investigation: [www.fbi.gov](http://www.fbi.gov)

-Awareness of National Security Issues and Response Program: [www.fbi.gov/hq/nsd/ansir/ansir.htm](http://www.fbi.gov/hq/nsd/ansir/ansir.htm)

-Critical Incident Response Group:  
[www.fbi.gov/hq/isd/cirg/cirgmain.htm](http://www.fbi.gov/hq/isd/cirg/cirgmain.htm)

Federal Emergency Management Agency: [www.fema.gov](http://www.fema.gov)

-Preparedness Training & Exercises: [www.fema.gov/pte](http://www.fema.gov/pte)

Joint Program Steering Group, U.S. Department of Justice and U.S. Department of Defense, Defense Advanced Research Projects Agency: [www.darpa.mil](http://www.darpa.mil)

National Criminal Justice Reference Service:  
[www.ncjrs.org](http://www.ncjrs.org)

National Domestic Preparedness Office: [www.ndpo.gov](http://www.ndpo.gov)

National Law Enforcement and Corrections Technology Center system: [www.justnet.org](http://www.justnet.org); [www.nlectc.org](http://www.nlectc.org)

Office of Justice Programs, U.S. Department of Justice:  
[www.ojp.usdoj.gov](http://www.ojp.usdoj.gov)

-Bureau of Justice Assistance: [www.ojp.usdoj.gov/bja](http://www.ojp.usdoj.gov/bja)

-Bureau of Justice Statistics: [www.ojp.usdoj.gov/bjs](http://www.ojp.usdoj.gov/bjs)

-National Institute of Justice: [www.ojp.usdoj.gov/nij](http://www.ojp.usdoj.gov/nij)

-Critical Incident Technology Program:  
[www.ojp.usdoj.gov/nij/sciencetech/counter.htm](http://www.ojp.usdoj.gov/nij/sciencetech/counter.htm);  
[www.justnet.org/techproj](http://www.justnet.org/techproj)

-Office of Science and Technology:  
[www.ojp.usdoj.gov/nij/sciencetech/welcome.html](http://www.ojp.usdoj.gov/nij/sciencetech/welcome.html)

-Office for Domestic Preparedness:  
[www.ojp.usdoj.gov/odp](http://www.ojp.usdoj.gov/odp)

-Office of Juvenile Justice and Delinquency Prevention:  
[www.ojjdp.ncjrs.org](http://www.ojjdp.ncjrs.org)

-Office for Victims of Crime: [www.ojp.usdoj.gov/ovc](http://www.ojp.usdoj.gov/ovc)

Office of Law Enforcement Standards:  
[www.eeel.nist.gov/oles](http://www.eeel.nist.gov/oles)

Office of Law Enforcement Technology Commercialization: [www.oletc.org](http://www.oletc.org)

Technical Support Working Group: [www.tswg.gov](http://www.tswg.gov)

U.S. Department of Defense: [www.defenselink.mil](http://www.defenselink.mil)

U.S. Secret Service: [www.treas.gov/usss](http://www.treas.gov/usss)

### **Websites for Non-Federal Institutes, Organizations, and Programs**

ANSER Institute for Homeland Security:  
[www.homelandsecurity.org](http://www.homelandsecurity.org)

Institute for Intergovernmental Research: [www.iir.com](http://www.iir.com)

-Regional Information Sharing Systems Program:  
[www.iir.com/riss](http://www.iir.com/riss)

-State and Local Anti-Terrorism Training Program:  
[www.iir.com/slatt/default.htm](http://www.iir.com/slatt/default.htm)

Institute for Security Technology Studies, Dartmouth College: [www.ists.dartmouth.edu](http://www.ists.dartmouth.edu)

Law Enforcement, Emergency Management, and Corrections Training Resources: [www.lectr.org](http://www.lectr.org)

National Domestic Preparedness Consortium:  
[www.emrtc.nmt.edu/events/ndpc](http://www.emrtc.nmt.edu/events/ndpc)

National Emergency Management Association:  
[www.nemaweb.org/index.cfm](http://www.nemaweb.org/index.cfm)

## ***How to order publications and videos***

Each publication and video entry includes a colored square indicating that it is available from either the National Criminal Justice Reference Service (NCJRS) or the National Law Enforcement and Corrections Technology Center (NLECTC). Publications and videos that have \* may be ordered by calling 800-851-3420; many NCJRS publications may also be downloaded from the Justice Information Center at [www.ncjrs.org](http://www.ncjrs.org). Publications and videos that have \*\* may be requested by calling 800-248-2742. These publications can be downloaded from JUSTNET at [www.justnet.org](http://www.justnet.org).

## ***How to find information at Internet sites***

Because the content and organization of websites change fairly often, the addresses or URLs listed will most often take users to the top-level home page of the site. In general, to find more specific information, users will have three options: (1) explore the site using the navigation buttons available on its home page, (2) search the site using its search engine (usually a link from or button on the home page), or (3) look through a site map (a page that lists all pages on the site).

***If you need additional assistance in locating any of these resources, contact the National Law Enforcement and Corrections Technology Center in Rockville, Maryland, at 800-248-2742, or e-mail [asknlectc@nlectc.org](mailto:asknlectc@nlectc.org).***

New Mexico Weapons of Mass Destruction Working Group: [www.wmd-nm.org](http://www.wmd-nm.org)

Oklahoma City National Memorial Institute for the Prevention of Terrorism: [www.mipt.org](http://www.mipt.org)

WMD First Responders.com:  
[www.wmdfirstresponders.com](http://www.wmdfirstresponders.com)

**The National Law Enforcement and  
Corrections Technology Center System  
Your Technology Partner**

***[www.justnet.org](http://www.justnet.org)***  
**800-248-2742**



This article was reprinted from the Winter 2002 edition of *TechBeat*, the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96-MU-MU-K011, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.