

THE EROSION OF LAW ENFORCEMENT INTELLIGENCE AND ITS IMPACT ON THE PUBLIC SECURITY

HEARINGS
BEFORE THE
SUBCOMMITTEE ON
CRIMINAL LAWS AND PROCEDURES
OF THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
NINETY-FIFTH CONGRESS
FIRST SESSION

PART 2

SEPTEMBER 28, 1977

Printed for the use of the Committee on the Judiciary

NCJRS



JUL 24 1978

ACQUISITION

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1978

49011

COMMITTEE ON THE JUDICIARY

JAMES O. EASTLAND, Mississippi, *Chairman*

JOHN L. McCLELLAN, Arkansas	STROM THURMOND, South Carolina
EDWARD M. KENNEDY, Massachusetts	CHARLES McC. MATHIAS, Jr., Maryland
BIRCH BAYH, Indiana	WILLIAM L. SCOTT, Virginia
ROBERT C. BYRD, West Virginia	PAUL LAXALT, Nevada
JAMES ABOUREZK, South Dakota	ORRIN G. HATCH, Utah
JAMES B. ALLEN, Alabama	MALCOLM WALLOP, Wyoming
JOSEPH R. BIDEN, Jr., Delaware	
JOHN C. CULVER, Iowa	
HOWARD M. METZENBAUM, Ohio	
DENNIS DECONCINI, Arizona	

SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES

JOHN L. McCLELLAN, Arkansas, *Chairman*

JAMES O. EASTLAND, Mississippi	STROM THURMOND, South Carolina
EDWARD M. KENNEDY, Massachusetts	ORRIN G. HATCH, Utah

PAUL C. SUMMITT, *Chief Counsel*
D. ERIC HULTMAN, *Minority Counsel*

THE EROSION OF LAW ENFORCEMENT INTELLIGENCE— CAPABILITIES—PUBLIC SECURITY

WEDNESDAY, SEPTEMBER 28, 1977

U.S. SENATE,
SUBCOMMITTEE ON CRIMINAL LAWS AND PROCEDURES
OF THE COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met, pursuant to notice, at 11:30 a.m. in room 3110, Dirksen Senate Office Building, Senator Orrin G. Hatch (acting chairman of the subcommittee) presiding.

Staff present: Richard Schultz, counsel; Robert J. Short, investigator; and David Martin, analyst.

Senator HATCH. The subcommittee will come to order.

Today's hearing is part of the subcommittee's ongoing investigation into the erosion of law enforcement intelligence and its impact on the public security.

In the course of this investigation, it has been brought to the subcommittee's attention that the erosion of law enforcement intelligence has seriously affected the ability of industry and business concerns to implement effective personnel security and corporate security programs.

To find out how serious and how widespread the problems were, the subcommittee established contact with the American Society for Industrial Security, an organization which I believe embraces the substantial majority of professional security officers in the private sector.

The subcommittee is grateful to the American Society for Industrial Security for its cooperation in bringing together the panel of security experts who are participating in today's hearing.

Our witnesses today are, in the order in which they will testify:

Mr. Donald Duckworth, director of corporate security for the Norton Co., Worcester, Mass. Mr. Duckworth also serves as chairman of the Committee on Privacy of the American Society for Industrial Security.

Mr. Henry Englisch, assistant secretary in charge of security of the Insurance Company of North America's Marine and Aviation Services, Philadelphia, Pa. Mr. Englisch is chairman of the Transportation and Security Committee of the American Society for Industrial Security.

Mr. Thomas Ruane, security manager of Avon Products, New York, N.Y., and a regional vice president of the American Society for Industrial Security.

Mr. Lindsay L. Baird, a private consultant on computer security, who also serves as chairman of the Computer Security Committee of the American Society for Industrial Security.

And Mr. Jan Larsen, manager of corporate security for the Pfizer Co., New York, N.Y.

Gentlemen, we are most grateful to you for coming here. I have only one observation to make before we take your testimony.

It has become a popular pastime on the part of certain elements in our society to downgrade private enterprise, to bait big business, and to regard the special problems that confront our business corporations as things divorced from the interests of the American public. It is my conviction, however, that no such divorce exists.

In the field of security, especially, it is obvious that what affects the security of private enterprise impinges in a direct and palpable manner on the welfare and security of the American people.

A terrorist attack on a utility company or an oil pipeline could impose untold suffering on millions of Americans.

Similarly, a terrorist attack on a major industrial computer center could conceivably put scores of thousands of Americans out of work.

The American people also pay for every cargo that is hijacked, for every act of embezzlement or pilferage by dishonest employees, and for the enormously increased security costs resulting from the breakdown of personnel security programs. They pay these costs for the simple reason that they have to be passed on to the consumer.

Your testimony, I know, addresses itself to all of these problems.

Gentlemen, before we proceed with your testimony, will you all rise and be sworn as a group?

Do you swear to tell the truth, the whole truth, and nothing but the truth so help you God?

Mr. LARSEN. I do.

Mr. RUANE. I do.

Mr. DUCKWORTH. I do.

Mr. BAIRD. I do.

Mr. ENGLISCHI. I do.

Senator HATCH. Our first witness is Mr. Donald Duckworth.

The hearings that we've held in this subcommittee have been startling as we've gone into various problems in the matter of law enforcement intelligence and its impact on the public security.

We're very interested in the testimony that you folks have to give today. It will be printed and disseminated. Some of the testimony that has been given in the past has, I think, done the American people a great service, because it has been printed and circulated. People in this country are starting to realize some of the disadvantages that everybody in this country is presently undergoing as a result of the lack of security information and the erosion of intelligence enforcement activities in our country, caused by the misapplication and misinterpretation of certain laws—or caused by laws that are, in themselves, too stringent under the circumstances.

So we want to welcome you to this subcommittee, and we will be very appreciative to have all of your testimony.

Mr. SCHULTZ. Mr. Duckworth, please proceed with your prepared remarks.

TESTIMONY OF DONALD R. DUCKWORTH, CHAIRMAN, PRIVACY AND INFORMATION MANAGEMENT COMMITTEE, AMERICAN SOCIETY FOR INDUSTRIAL SECURITY

Mr. DUCKWORTH. Thank you.

Mr. Chairman and members of the subcommittee, I am Donald R. Duckworth, chairman of the Privacy and Information Management Committee of the American Society for Industrial Security.

My appearance at this time is on behalf of the officers, directors, and members of the American Society for Industrial Security—commonly referred to as ASIS—concerning the impact on security programs in private and public organizations of the erosion of law enforcement intelligence-gathering capabilities.

Security programs in private and public organizations are designed and maintained to protect the personnel, facilities, information, and other assets necessary to accomplish the purposes for which an organization is operated.

By purpose and design, these security programs aim to provide protection primarily by prevention of loss, by prevention of unlawful activities, as well as prevention of fires and accidents.

ASIS is a professional society founded in 1955 of security executives and administrators in over 3,000 business, industry, and government—education, financial, and health care—organizations having requirements for security and loss prevention programs for the protection of personnel, information, facilities, and other assets.

Our worldwide membership currently numbers 10,000 individuals organized in 102 chapters—both in the United States and other international areas.

Our society, as an organization, does not espouse a particular position or give testimony on public issues unless:

First, the special knowledge and experience of the professionals in the field of security is directly applicable to the issue.

Or, second, the programs for the protection of assets and personnel, which are the managerial responsibility of security professionals, are directly affected.

We feel the society's contribution to the development of public issues is most valuable by identification of members whose programs and organizations, whose knowledge and firsthand factual experience, are most pertinent to a particular issue.

Then, by encouragement and liaison efforts, we bring them together with other disciplines, organizations, and public officials for the interchange that can produce increased understanding and better decisions by all parties concerned.

Consistent with that usual role, we have worked to assist this present hearing through members and their organizations who are seriously concerned with the adverse impacts on time-tested security and loss prevention programs, of the erosion of law enforcement intelligence-gathering capabilities; and who, at the same time, based on direct

knowledge and experience gained in operating such programs, are able and well qualified to cite and illustrate the practical effects of decreased capabilities in intelligence-gathering functions of public law enforcement agencies.

We appreciate the opportunity to be here today to convey the security professionals' general, great concern as to the serious consequences of adverse development affecting law enforcement intelligence-gathering capabilities.

Based on our memberships' special area of experience, as well as general public experience of events in our world today, we envision two major adverse consequences if intelligence-gathering activity and information by authorized law enforcement agencies is less than adequate to prevent or protect against criminal threats that realistically exist.

One consequence of less-than-adequate capabilities would be a crippling impact on the effectiveness of security and loss prevention programs in business, industry, and government.

The further consequence we project, if the effectiveness of programs which protect people and property are reduced, is that it will become increasingly difficult, even doubtful, that the basic values necessary for the general welfare and for economic growth in a free society can be preserved.

That concludes my statement, Mr. Chairman.

ASIS is most grateful for the opportunity afforded to appear and provide this background to the specific information that security professionals and the companies they represent are well qualified to supply on the issue under consideration by this subcommittee.

Mr. SCHULTZ. We thank you for your statement, Mr. Duckworth, on behalf of ASIS.

If we may, let's move to the statement of Mr. Englisch and give you a little breather before you present your other prepared remarks.

Mr. ENGLISCH, would you proceed?

TESTIMONY OF HENRY ENGLISCH, SECRETARY, MARINE AND AVIATION SERVICES, INSURANCE CO. OF NORTH AMERICA, PHILADELPHIA, PA., AND CHAIRMAN OF THE TRANSPORTATION AND SECURITY COMMITTEE OF THE AMERICAN SOCIETY FOR INDUSTRIAL SECURITY

Mr. ENGLISCH. Thank you.

I am honored by the invitation to appear before the Senate Subcommittee on Criminal Laws and Procedures to express my beliefs regarding the erosion of law enforcement intelligence and its impact on the public security.

Constrained in my personal area of security experience to the subject of transportation security, primarily the security of goods in transit, I will restrict my contributions to those areas.

My primary duties at present involve the guidance and direction of a field force of transportation specialists who, among other duties, provide consultative services to shippers and carriers insured by my company in a continuing effort to reduce the loss of cargo in transit.

As physical security of cargo is a significant part of our working considerations, I have become a member of the American Society for Industrial Security.

Having served 3 years on the Transportation Security Committee of the society, I am presently chairing the committee.

In 1976, I was appointed a member of the National Cargo Security Council, a counterpart group of the Interagency Committee on Transportation Security—ICOTS—chaired by the Department of Transportation.

The council provides the interagency group with viewpoints of the private sector regarding transportation security.

I am also a member of the Cargo Loss Committee of the American Institute of Marine Underwriters.

In these three related areas of activity, it has become increasingly apparent to me that the erosion of law enforcement intelligence has had a deleterious effect on the maintenance of transportation security.

Considering cargo security, it is evident that theft-related loss of goods in transit is an area of major loss. From my company's experience alone, we estimate that some 33 percent of cargo loss is related to theft.

I would like to interject a comment here raised on a publication of the company that is afforded to shippers, carriers, and interested parties. It gives a statistical breakdown of loss in cargo, which has been compiled by my company alone.

While it doesn't cover the entire industry, we feel our experience is significant and large enough to make this a valid indication of the cargo loss statistics.

Mr. SCHULTZ. Would you identify the source of the data?

Mr. ENGLISCH. This was published 2 years ago. A new copy is in progress right now.

Mr. SCHULTZ. From which page will you be quoting?

Mr. ENGLISCH. Page 38 of the publication: "Ports of the World," 10th edition.

Mr. SCHULTZ. Thank you.

Mr. ENGLISCH. We feel, also, that a considerable portion of cargo theft is a result of collusive effort between employees of transportation companies and between those employees and employees of cargo shippers and receivers. Of course, and not to be excluded, are employees of periphery industries, such as insurance companies and agents, cargo brokers and banks—all of whom have access to cargo, insurance, and credit documents which in turn can be used for hijacking, theft, and pilferage purposes.

In this connection, availability of criminal record information on prospective employees is, in my opinion, essential to transportation industry employers.

Further, the efforts of law enforcement agencies in combating cargo crime are rendered less than effective due to the deterioration of intelligence exchange between the agencies.

Cargo in transit can be simultaneously local, interstate, and international in nature.

It is relatively easy to recognize that employee collusion can extend across city, State, and National boundaries.

Accordingly, criminal information intelligence from many jurisdictional sources is vital to the effective control of cargo theft.

Perhaps an example would be pertinent.

A high-value air cargo shipment destined to a European consignee may well be subject to a number of en route landings and even an exchange between carrying airlines before arriving at a destination.

Through collusive effort, a conspirator at an on-the-way stop, having been notified of the presence of the target shipment on a particular flight, could effect removal of that shipment for later disposal. The loss would not be evident until the aircraft arrived at a distant transfer or delivery point.

It is obvious that cooperation between law enforcement agencies in widely separated cities and States is essential to the prevention and control of this type of crime.

The lack of free and responsive transmission of criminal intelligence in these situations can only serve to make the efforts of criminals more effective.

When one realizes that a considerable amount of what could be termed sensitive cargo is constantly in transit in all transport modes, it becomes evident that with limited security capabilities, the purposes of terrorist groups may well be served.

Nuclear fuels and explosives are examples of cargoes that could be seized and used for terrorist activity or extortion purposes.

Just a few weeks ago we had a situation in the State of Florida in which a pesticide was introduced into a municipal water system with fortunately no deaths involved to my knowledge, but a situation of great consequence.

The ability to obtain quantities necessary for this type of terrorist and extortion activity usually rests in the transportation act—where due to lack of security a similar material might be obtained from a rail car, a platform, or through collusion with an employee of the shipping and transportation company.

This alone, in my opinion, is significant enough to warrant close scrutiny of the hazardous materials in the transportation chain to insure that they do not get to unauthorized persons.

All transport modes—rail, motor, air, and marine—are subject to the cargo theft problem. But even greater hazards exist—those which include disruption or destruction of transportation facilities—which could be perpetrated for extortion or terrorist purposes or to interdict defensive efforts on the part of our military forces.

Recognizing the gravity and impact of interference with the uninterrupted flow of passengers and cargo over our national transportation network and through its interfaces with the international transportation systems, every possible effort must be made to insure the security of those systems.

Employees of the transport industry are frequently entrusted with the safety and security of literally hundreds of lives and major dollar values at any given time.

I submit that this special trust is of a magnitude and gravity rarely matched in other industries. Accordingly, the confidence placed in these employees by the public must be based on the highest order of proven reliance and competence.

Our law enforcement agencies must be permitted maximum reasonable latitude in the development, exchange, and use of criminal intelligence in connection with activities which may interfere with the secure operation of our national transportation facilities.

This latitude must extend to prior criminal activities of employees of transportation and periphery industries and to the current activities of individuals, organizations, and groups impacting on or threatening the physical flow of commerce.

A free, rapid, and continuing exchange of criminal intelligence between law enforcement agencies at all jurisdictions—local, State, national, and international—is crucial to the safety and security of the people of the United States of America.

Mr. SCHULTZ. Mr. Englisch, could you give us a few more details on the Florida extortion case?

Mr. ENGLISCH. At the present time I'm only aware that the situation occurred. There apparently was a commercial pesticide, which is usually labeled as a hazardous cargo, depending on its nature. It was apparently obtained by the people who perpetrated the case, and at this time it's under investigation. That's as much as I can offer.

Mr. SCHULTZ. There wasn't extortion involved or a money demand made?

Mr. ENGLISCH. Not that I know of. That's correct.

Mr. SCHULTZ. Has there been an arrest in the case?

Mr. ENGLISCH. Not yet.

Mr. SCHULTZ. What is the extent of the injuries, if you know?

Mr. ENGLISCH. There were no injuries indicated. But tainting of a city's municipal water supply immobilizes this resource, and there are very significant expenses until it's cleaned up. It might be termed a near-miss.

Mr. SCHULTZ. Thank you.

Mr. Duckworth, we will return to you for your statement as representative of the Norton Co.

Mr. DUCKWORTH. Thank you, Mr. Schultz.

I wish to thank the subcommittee for this opportunity to express my views on the erosion of law enforcement intelligence capabilities and the impact that this erosion has had on the security function in the private sector.

For you to truly gain an appreciation and understanding of my perspective and the views which I will present this morning, I believe that it is incumbent upon me to provide you with some insight into the business which I represent as well as the nature of the function which I perform in that organization.

Norton Co. is a multinational industrial manufacturer with 23,000 employees and 110 plant locations in 26 countries. It is the world's leading manufacturer of abrasives and abrasive products, the world's largest maker of diamond drilling and coring bits for gas and oil exploration, and the leading maker of diamond mining products in the United States.

Other products include personal safety equipment, insulating sealants, medical, and scientific plastic components, chemical process products, and industrial ceramics.

Norton's 1976 total sales were \$750 million.

Now that you have some understanding of the organization in which I work, let me take you into the world of the corporate security director and acquaint you with what I do and how I do it in that world.

Before proceeding, let me preface my comments by stating that the basic functions which I am about to describe are not unique to me or Norton Co.

Although techniques, methodologies, and managerial emphasis often vary widely from company to company, I am confident that the basic objectives and principles of the security function which I will describe are generally illustrative of and applicable to the vast majority of security executives within the private sector today.

I believe that I can best begin this odyssey by quoting from the introductory paragraph from Richard Cole's text: "Protection Management and Crime Prevention."

The protection executive, contrary to mass opinion, is not a private protector of the law who titillates the imagination of the general public with his courageous deeds. He is instead a business executive given the job of protecting corporate assets. His most definite and challenging responsibility is predicting the opportunities for the loss of corporate assets and reducing those opportunities to manageable proportions.

Gentlemen, this is a point which I cannot overstress.

I do not, nor in my opinion do any of my colleagues, view ourselves as part of the criminal justice system and I do not appear before you in any implied or quasi-law enforcement role.

Rather I appear before you, first and foremost, as a professional business manager—albeit, one with a rather unique and esoteric specialty.

However, the terms that I normally deal in are those of risk management, cost effectiveness, return on investment, and profit and loss—all terms of the business world.

As the staff executive in my company with the responsibility for development of a protection program for our entire enterprise, both domestically and internationally, you will more often find me behind a desk formulating policy statements than involved in some form of investigative derring-do in conjunction with some law enforcement agency.

The essence of the functions which I perform centers around:

First, an identification of the security vulnerabilities of various categories of corporate assets to loss;

Second, an assessment of the probabilities of those losses occurring;

Third, an evaluation of the criticality, generally in financial terms, to the organization if one of those losses occurred;

And, fourth, after relating these factors, the development of specific countermeasures, ranging from sophisticated and costly computer-based alarm systems to the utilization of security guards to prevent losses from occurring.

The emphasis of the function, then—and I cannot stress this point too highly—is that of prevention, and the scope is as all-encompassing as those multitudes of conditions which may result in asset loss.

Inherent in this loss-prevention approach is the never-ending need for information.

I talked a few moments ago about security vulnerability probability, and criticality with the end result being the development of security countermeasures to prevent loss from occurring. Crucial to the successful development of these countermeasures is an accurate assessment of the first three, which can only be obtained through information.

Again, bear in mind that just as I am concerned about loss resulting from criminal activity, so too am I equally concerned about loss resulting from such diverse conditions as fire, explosion, hurricanes, tornadoes, and so on.

This same thought also holds true in my need for information. Not only am I concerned about the availability of information which can assist me in preventing loss from the criminal act, but I am equally concerned about such diverse information as weather forecasts, fire protection data, and so forth.

At this point, I can only hope that your concept of the corporate security director is seen in the context of the businessman legitimately preoccupied with a task of asset protection accomplished through loss prevention techniques.

Before leaving this discussion of the nature of the security function in the private sector, I would like to make one final point concerning a basic principle of security adhered to by the majority of security practitioners.

It can best be made by quoting from Knight and Richardson's text:

THE SCOPE AND LIMITATION OF INDUSTRIAL SECURITY

No property right takes precedence over personal liberty or dignity, simply because the property right is based upon personal liberty and dignity and not vice versa.

However, there is no necessary conflict of interest in this particular. The property right can be safeguarded and the individual dignity preserved by the adherence of each to its proper prerogatives.

As for the security function, it must base the design of its control upon a given view of the nature of the human person or personality—and be careful to avoid a surreptitious psychological reversal of the order of precedence.

At this point, it now seems appropriate to focus my comments on the one condition which, in terms of probability and criticality, generates our most serious vulnerabilities and is, of course, the very reason for our being here today.

The condition is obviously crime and, more specifically, the significance of crime and its infinite variations as a threat to American business today.

I contend that, because prevention is such a vital part of the work of the security professional, I cannot meet my responsibilities and protect the assets of the company that I work for without access to needed facts about crime and criminals.

In particular, there are three extremely crucial criminal threats about which I need to receive information in order to effectively perform my duties—terrorism, organized crime, and technology theft.

I will address each of these areas separately, but first let me tell you of the position that I, as a practicing security professional, find myself in today.

There is not one criminal justice agency with which I deal—and these range from local municipality police forces to Federal investigative agencies—that is not prohibited from furnishing information to the private sector, with but exceedingly limited statutory exceptions.

The erosion of law enforcement intelligence capabilities, especially as it impacts upon the private sector, quickly becomes a moot point to be debated internally within the law enforcement community as far as the private sector is concerned.

As a Fortune 500 manufacturer with a diversity of products, my company represents several potentially special target areas in which the absence of knowledge about those who might commit crimes, as well as the nature of the criminal activity itself, is dangerous to the point of being foolhardy.

Yet we have no formalized information exchange. Police often are able to identify new crime trends but generally have no way to provide that information to those in industry who might benefit from it.

Last week, in preparation for my appearance here today, I queried several officials of law enforcement agencies, ranging from local to Federal, with which I maintain close liaison to determine their thoughts in this area.

All unanimously agreed on the following points:

First, their intelligence-gathering capabilities had been drastically reduced—in some cases, to the point of being nonexistent.

Second, this reduction or erosion in their intelligence capabilities was generally attributed to a combination of the four causes identified on page 11 of the annual report of the Internal Security Subcommittee for the fiscal year ending February 28, 1977.

Third, the primary reason mentioned was the enactment of the Freedom of Information Act and the Privacy Act.

Fourth, information developed concerning a specific threat directed against my company would generally be passed only if there was a "clear and immediate" danger.

And, fifth, there should be some institutionalized method for information transfer between the police community and the private sector due to the commonality of interest.

Consequently, I have two real concerns today. My first and most imperative is that of the need for intelligence to enable me to anticipate and prevent crime in the performance of my job.

The second concern is more general but just as real. A concern that law enforcement intelligence capabilities have been weakened to the point that they can no longer even warn me of a "clear and immediate" threat which places corporate assets, to include people, in immediate jeopardy.

Logic seems distorted when, in the face of rising crime and the inability of traditional measures to deal with that fact, the business community is effectively foreclosed from taking limited but meaningful action designed to prevent crimes, not invade privacy.

No better example illustrates this point than that of terrorism. Although terrorism represents only a small portion of the crimes committed against business, its very nature evokes a visceral reaction quite different from other forms of crime, and the corporate organization finds itself vulnerable to this threat throughout its operations.

Several months ago, a series of bombings occurred in Massachusetts. One, in particular, was directed against a major company, allegedly because of its business involvement in South Africa.

Since Norton Co. also has business interests in South Africa, it seemed logical that we also might be confronted with this type of incident.

When local, State, and Federal law enforcement agencies were questioned about the nature of the threat, the probability of additional bombings, the likelihood of us being a potential target, sus-

pects' identities, description of perpetrators—in short, any information which would assist in an effective development and implementation of additional countermeasures—the same old refrain was heard: No information available, probably couldn't be released if it was available, no intelligence-gathering capability existing, intelligence unit disbanded, reduced, ineffective. In short, no information collected and none available.

A terrorist could have gone to work for us that day for the express purpose of infiltrating our organization, preparing intelligence data on the target—us—and assisting in the execution of the terrorist act.

In all probability, I would have never known it and the countermeasures which have been painstakingly thought out would have been totally ineffective, simply as a result of our being unable to develop accurate, credible information on the threat.

The area of organized crime is very similar. Like other major companies, we do business with a wide variety of concerns ranging from the very small to the very large.

We recognize the widespread existence of organized crime and its increasing trend to use legitimate businesses as fronts and covers for illegal operations as well as to launder dirty money.

However, in today's climate, it is practically impossible to do anything other than worry since we are in a position of recognizing the general threat but unable to obtain any information to counter any specific threats that might be posed against Norton Co.

Let me give you another specific example to indicate why I feel that my fear is real.

Recently, during the process of performing a routine review of a small concern which we were contemplating using to establish a national manufacturer's representative system for a particular product line, it was discovered that one of the principals in the firm ran afoul of the legal system and was currently on probation for a number of years after having pled guilty to several counts of falsifying accounts receivables to illegally obtain loans.

That much was part of the open record and obviously raised many legitimate concerns on our behalf about the reputability and integrity of the principal and his company.

Upon a further in-depth review, the principal provided a perfectly plausible reason for the action which, although not justifying the action, certainly provided some major mitigating and extenuating circumstances.

However, the overall picture developed as a result of our investigation efforts also fit the classic picture of organized crime involvement.

Result : The perfect dichotomy. Solution : None.

When we attempted to move out of the open court records and further explore the situation through law enforcement agencies, we were stymied.

The same old refrain: No information available; if it was, not feasible.

I again ask the rhetorical question: How can you effectively prevent loss of assets from criminal activity if you are unable to determine that there is, in fact, criminal activity?

Technology theft also presents us with a very real threat and corporate fear. Our information and proprietary processes are the very lifeblood of our business and often represent the competitive edge which we enjoy in the marketplace.

Additionally, some of this very same technology is also vital to our national defense.

A recent article by Clarence M. Kelley, Director of the Federal Bureau of Investigation, on the subject of domestic industrial espionage stated:

In summary, the threat of espionage efforts, foreign and domestic, against American industry represents a very real danger. The FBI will vigorously combat this threat within its jurisdiction; however, it is incumbent upon American industry to strengthen its own defenses against all espionage acts inimical to its own and the nation's interest.

Believe me, we would like nothing better.

Again the dichotomy. We recognize the general threat but are hampered from obtaining information which would enable us to develop the specific threats, the knowledge of which is essential for effective security planning.

Let me provide yet another example to demonstrate our paradox.

An emigre from an Eastern Bloc country goes to work for Norton Co. in an abrasives engineering position. The position is basically an entry level one, and the individual obtains the position based upon an application indicating some rudimentary education and experience in this area.

The position is basically nonsensitive in that it does not provide access to proprietary information or processes, and it does not provide access to classified defense information.

After several months in the job, performing in an acceptable manner, the individual is considered for a position which will provide access to proprietary technology, although not defense information.

About this same time, reports are passed to the security director indicating that the individual in question appears to have a far greater understanding of abrasives technology than was earlier apparent from his resume and work experience.

Exceptionally qualified employee or industrial spy? Who knows?

It is almost impossible to obtain any information or intelligence on this individual. The only way that I could visualize any type of background check being accomplished by a Federal investigative agency would be in the event that the person would require access to classified defense information.

In today's modern business environment, especially in the company that operates on an international basis, this type of incident is all too often the norm, and we often find the situation even more ambiguous due to the complexities of the environment.

Current restrictions on law enforcement intelligence capabilities, combined with the lack of formalized information exchange needed by the private sector, all but ties our hands in cases like this and often does a disservice to both the company and the individual.

Let me conclude my remarks by stating that as a member of the business community, especially as a member charged with protection of his company's assets who, while not a public law enforcement

officer myself, feel that I still have a real and legitimate need to know if criminally inclined individuals are encroaching upon my company's sphere of activity.

I do not feel that the right of my company to protect its assets by trying to anticipate and prevent crime is mutually exclusive with the individual's right to privacy. To this end, I am deeply concerned about the dangerous erosion of law enforcement intelligence capabilities, especially because of the impact that this erosion has on an already-grim situation.

If corporate security efforts can be identified as a form of business crime prevention and crime prevention can be defined as the anticipation, recognition, and appraisal of criminal threats, and then the initiation of specific action to remove or reduce them, then I believe that you too will share my concern since we will be unable to do it without a strong information flow.

In William K. Lambie's book, "The Defenseless Society," he makes this point quote eloquently.

There is a whole segment of our society that * * * between them they have put shackles on legitimate anti-crime efforts that are reflected not only in escalating crime statistics but in the succession of roadblocks thrown in the way of all those who are trying to do their jobs more effectively.

If they are successful, we may be able to live with the society that results, but it will most assuredly be a defenseless society.

Thank you.

Mr. SCHULTZ. Thank you, Mr. Duckworth.

That was a very thoughtful statement and somewhat provocative. It will prompt questions later which we will address to the full panel.

Mr. Ruane, would you proceed at this time?

TESTIMONY OF THOMAS F. RUANE, JR., REGIONAL VICE PRESIDENT,
AMERICAN SOCIETY FOR INDUSTRIAL SECURITY, FORMER INVESTIGATOR,
U.S. POSTAL INSPECTION SERVICE, AND CURRENTLY CORPORATE MANAGER OF SECURITY,
AVON PRODUCTS, INC., NEW YORK, N.Y.

Mr. RUANE. Thank you.

My name is Thomas F. Ruane, Jr., regional vice president, ASIS—the American Society for Industrial Security. I am a former investigator for the U.S. Postal Inspection Service and am currently corporate manager for security for Avon Products in New York.

Mr. Chairman, I would like to take this opportunity to thank the Senate subcommittee for their invitation to testify at these hearings on the erosion of law enforcement intelligence and its impact on the public security.

There is no direct impact on public security because, in the past, prior to Freedom of Information Act and Privacy Act of 1974, few agencies in the Federal Government disseminated any intelligence to the private sector without court orders or signed releases from the interested parties.

The public security concern is what has happened to intelligence-gathering since the Freedom of Information Act and the Privacy Act of 1974.

There is a definite need for clarification on many parts of this legislation. There are too many gray areas in the interpretations of what can be gathered and what cannot.

I have heard from some Federal agency sources that they do not collect any type of intelligence any more because at least that way you cannot get into trouble. This attitude can affect the future security of every citizen.

Terrorism has become a major concern to national and multi-national companies, and they would like law enforcement to have as much intelligence as can be obtained; hence, I hope that this type of intelligence is being collected and documented.

The Departments of State and Commerce have done an outstanding job in this area in the past with a direct result being the saving of countless lives and untold millions of dollars in property damage.

The use of informants has eroded considerably because of the possibility of exposure through the Freedom of Information Act.

Intelligence collected from informants by law enforcement agencies has been used to prevent dishonest acts against the Government and, in some cases, saved corporations loss of merchandise and money.

Prevention of crime has become the watchword in the world of private security as opposed to apprehension.

This crime prevention concept is the function of a whole new department in the Federal Bureau of Investigation. They have asked for the cooperation of industry to assist in the reduction of crime.

If such cooperation between Government and industry is accomplished—and I feel sure it will—there should be a marked reduction in white-collar crimes which has shown the largest statistical increase in the past 5 years.

Undercover investigation has eroded because of lack of funds to be used to make purchases of illicit merchandise from known felons. LEAA has funded many State and municipal law enforcement agencies for the creation of task forces against organized crime.

These groups have closed down large-scale illegal trafficking in automobiles, boats, and other artifacts. These groups have identified the participants in these illegal marketing schemes.

Presently, Federal Government agencies have minimal funds to carry on this type of intelligence so very little is being done. This is and should be a concern to all public security-minded citizens.

In summary, the importance of public security goes far beyond the points I have raised, but I would hope that in some small way I have provided some food for thought for your committee.

Thank you.

Mr. SCHULTZ. Thank you, Mr. Ruane.

TESTIMONY OF LINDSAY L. BAIRD, JR., INDEPENDENT SECURITY CONSULTANT AND NATIONAL CHAIRMAN OF THE COMPUTER SECURITY COMMITTEE, AMERICA SOCIETY FOR INDUSTRIAL SECURITY, WASHINGTON, D.C.

Mr. BAIRD. Thank you.

I appreciate the opportunity to appear before you and express my beliefs regarding the erosion of law enforcement intelligence capabilities and the actual/potential impact upon industry.

I have read both the annual report, Report No. 95-20, and the committee print entitled "The Trans-Alaska Pipeline" of the subcommittee to investigate the administration of the Internal Security Act and other internal security laws as well as the testimony of Glen D. King, executive director, International Association of Chiefs of Police—IACP.

I am in complete agreement with the concerns expressed by the witness whose testimony is contained in these documents.

I do not wish to restate problems that have already been addressed but rather to bring to your attention to an area of criminality that can and will have a profound impact upon the operational efficiency and profitability of industry. The topic I wish to address is white-collar crime—computer style.

I am very much concerned about our industry's ability, as well as all levels of government, to properly safeguard vital assets and highly private or economically valuable information. My concerns are the protection of computing systems from accidental, malicious, criminal, or unauthorized manipulation of systems, files, and data.

The Privacy Act of 1974 does and, I assume, the actions Congress may take on the recently released recommendations of the President's Privacy Protection Study Commission will have an adverse impact upon industry's ability to counter these threats.

A U.S. News & World Report article, June 13, 1977, "How the Mafia Invades Business," provides some insight as to the criminal intelligence needs of both law enforcement and industry.

Mr. Bullock, chief of the Illinois Bureau of Investigations, responded to the question: What's the next field for the organized criminal to conquer?

He responded as follows:

We know from our sources that figures in organized crime have expressed great interest in moving into computer fraud. They are taking a very, very strong look at it and they are prepared to move promptly. Someday we are going to read about one hell of a heist.

Mr. Bullock has justifiable concerns. The Department of Commerce estimates that current losses from computer fraud exceed \$100 million per year. I firmly believe, based on information developed in recent years, that actual annual losses may approximate \$1.5 billion in 1977.

The greatest vulnerabilities to the security of assets and sensitive information resident on computing systems are people.

The most secure physical environment offers little protection against dishonesty, deranged, or disgruntled employees. The only measures by which an individual can be evaluated are past and current performance in education, business, and society.

The Fair Credit Reporting Act and the Privacy Act of 1974 have impacted on our ability to determine the reliability of data processing employees, as well as all others, that fill positions of trust.

The Privacy Act of 1974 has all but sealed criminal records; however, industry has a legitimate and pressing need for selected criminal history information.

True, criminal history records are inaccurate and the release of nonfactual records can and does cause harm. However, would not our society as a whole be better off if all criminal justice agencies were required to maintain accurate records about an offender and the final

disposition of a case, as opposed to sealing or otherwise hiding an individual's criminal record in the name of privacy?

I believe that it is very important to speculate as to what the potential losses in the area of computer crime may be. No one knows the actual dollar losses of either assets and/or information experienced by industry or government.

I know from personal experience that industry is reluctant to report computer crimes to law enforcement agencies. The reasons given for not divulging criminal activity include embarrassment, loss of public image, and the potential for a stockholder's suit.

Computer manufacturers also do not want to announce the number of criminal attacks that have been made against their equipment configurations.

I believe most, if not all, computer manufacturers have, at one time or another, addressed the problem of computer crime. The customer engineers and other manufacturing maintenance technicians are usually one of the first persons a data process manager calls upon when a problem develops. Good, factual information is in all probability available; however, I doubt if it would be voluntarily disclosed by most.

In 1974, I cochaired a computer security seminar with a computer manufacturer's representative. During his presentation, he reported on the results of a year-long computer crime study his company conducted in 1973 for their own internal use. The results were alarming.

I took rather detailed notes on this presentation, and a year later I wrote to the speaker and asked him to confirm the accuracy of my notes.

This letter, dated October 7, 1975, as well as a second letter dated January 27, 1976, representing confirmation were not answered. Therefore, I cannot attest to the accuracy of my original notes. However, I have every reason to believe that they are correct.

My notes were as follows:

One, a study pertaining to dishonest employees in a data processing environment was conducted in 1973.

Two, between 20 and 30 events of dishonest activity were reported each month during this year-long study.

Three, the average per-event loss approximated \$674.300.

Four, 85 percent of the subjects identified in this study were not prosecuted.

Five, only one in five of the subjects referred to the courts received a sentence imposing confinement.

Six, the odds of a person going to jail are 1 in 33.

This study is very interesting in that a Mr. Don B. Parker, then with Stanford Research Institute, reported in 1973 on the results of his study into computer abuse.

Mr. Parker received a grant from the National Science Foundation to do a study on computer crimes.

He reported in November 1973 that his work to that date had developed information about some 148 incidents of computer abuse. The earliest incident occurred in 1964. Parker was able to obtain dollar-loss data for only 65 of these cases. The total losses were \$90,514,000. This equates to an approximate average loss per computer crime of \$1,392,000. It is noteworthy that the Equity Funding Life

Insurance fraud losses of some \$2 billion was not included in Parker's figures (Computer Abuse, by Don B. Parker, Susan Nycum & S. Steven Oura, November 1973, Stanford Research Institute).

It is important to note that Parker only found 148 incidents of computer abuse during his original study. This covers a time span of some 9½ years. However, the computer manufacturer's study indicates that not less than 240 nor more than 360 criminal events occurred during a 12-month period. This suggests that we are only seeing the tip of the computer-abuse iceberg and that we do not know the true dimension of the problem.

The February 23, 1976, edition of Crime Control Digest reported on a paper Mr. Parker prepared for delivery at the 142d annual meeting of the American Association for the Advancement of Science. In this paper he provides an update on his work in the area of computer abuse. I shall quote portions of this article:

Parker said that he had amassed a collection of 380 reported cases on computer abuse, including a case in which a programmer took a program from his competitor's computer over a telephone circuit.

Parker said his study, based on interviews with 17 "perpetrators," showed: Eight cases involved financial gain averaging \$500,000 per case and ranging from \$1,400 to \$1.500 million.

Half of these cases involved collusion. Eleven of the 17 held positions of trust.

Half the cases involved manipulation of data into or coming from computers. The others involved more technical efforts in which programs were changed and data manipulated within the computers.

For 15 of the perpetrators, their acts represented fascinating challenges. They looked upon their activities as a game with the computer system.

The perpetrators drew a line between hurting people, which they saw as immoral, and harming organizations, which they could easily rationalize.

Generally, the perpetrators were aggressive, eager, bright, quick-witted and gregarious. They exhibited all the characteristics that would make them highly desirable employees.

I have assumed that users of computing systems manufactured by vendors other than the one that conducted the study must have experienced similar criminal activity in proportion to their manufacturer's share of the national market.

The number of computing systems currently in use today are approximately five times as many as in 1973.

An article entitled, "Coming: Another Revolution in Use of Computers," appearing in U.S. News & World Report of July 19, 1976, is my source. I will provide a copy of that page.

The mathematics involved in computing the probable 1977 losses due to computer abuse are simple; however, the result is astonishing.

There are in excess of 680,000 computing systems in the United States today. Assuming that there were approximately 150,000 systems in 1973, one can extrapolate, after assigning several other assumed values, the expected number of criminal attacks on the current total computer population. These computations suggest that some 2,200-plus criminal events may take place this year, and the potential loss can reasonably be expected to exceed \$1.5 billion.

White-collar crime—computer-style—is a logical area to be exploited by organized crime and other groups.

The U.S. Senate, Committee on Governmental Operations, in its staff study of computer security in Federal programs, February 2,

1977, found two areas of computer operations which are in immediate need of improving security policies and procedures.

These problems are, first, those concerned with the distribution of funds; and, second, those which offer the opportunity to divert highly private or economically valuable data.

While this report deals with problems in Government, it does recognize that the private sector has similar problems—personnel and physical security. The committee also found that computer crimes, especially those which divert funds or economically valuable data, are likely to become the prevalent white-collar crime in the future.

I would like to emphasize that one statement.

The committee recommended that computing systems that distribute funds and/or process highly private or economically valuable data be categorized as critical-sensitive because of the harm or loss that could result from criminal abuse, unauthorized access, or manipulation of data.

A second recommendation calls for reform in personnel security practices to insure that qualified and trustworthy individuals are selected to work on sensitive computer operations.

In this instance, they are recommending that personnel working with Government critical-sensitive computing systems be subjected to an in-depth full-field background investigation.

The Federal Government is starting to recognize its vulnerabilities, and it has the statutory authority and resources with which to initiate corrective and protective measures.

However, we in the private sector are not that fortunate, as criminal records, criminal intelligence, accurate investigative consumer reports, factual prior employment history, et cetera, are either not authorized for release or are not readily available.

Our legislators have more than adequately protected the rights of the criminal community; however, they have not yet addressed the rights of their victims—both citizens and industry.

The May/June 1977, article in Computer Security—"You may have to hire alcoholics or drug addicts in the data center unless . . ." plus newspaper and radio reports on HEW's rules banning job discrimination against the handicapped concern me very much.

Handicapped, as I understand HEW's interpretation, includes alcoholics and drug addicts. Attorney General Griffin Bell ruled that these categories were, indeed, included as handicapped. Must we then have alcoholics and drug addicts working in critical-sensitive data processing positions that involve the distribution of funds and highly private or economically valuable data?

I trust and pray that this is not the case.

The Government may exempt its agencies from this mandate to hire the handicapped via the critical-sensitive designation; however, there are no such procedures that I know of that can be legally applied in the private sector.

Information about alcoholics, drug addicts, criminals, and so forth, is exceedingly difficult to obtain now; however, industry has a need and a right to know about the individuals that they place in positions of great trust.

The private sector needs information—factual criminal histories and consumer credit reports, selected criminal intelligence when it

may or will impact on a particular business, background data, and so forth—if it is to protect its assets.

The Congress and the courts have been overly concerned with protecting the rights of the misfits in our society. They now have more rights and privileges than honest, law-abiding citizens. It is about time someone started restoring the rights of both good citizens and industry to be safe and secure in their homes and businesses.

There is one more area of concern that I would like to address before I terminate my prepared remarks.

The subject is terrorism in data processing environments.

All too frequently we read in our newspapers and view with disgust on television the barbaric actions of terrorist groups throughout the world.

In my judgment, what we are currently reading and seeing is but the tip of the iceberg. Both industry and Government are becoming more and more dependent upon computing systems for their day-to-day activity. I can no longer speak with authority about Government's dependence upon computer resources; however, I can address industry's dependence upon this singular resource for efficient and profitable operations.

The total loss of computer power for a period of 3 to 5 days can reasonably be expected to have catastrophic impact upon many companies. The severity of any interruption in the availability of this business tool increases at unbelievable rates the longer systems are disabled or unavailable for normal operations.

It is my firm belief that we will witness within a relatively short time an attempt by an activist group to achieve their ends, whatever they may be, by either holding a corporate computing system hostage or destroying a critical subset of a system with threats of disabling other components.

Italy within the past 12 or 13 months has been subjected to 10 attacks against corporate and Government computer centers by armed terrorist groups.

A front page article in Computerworld, August 29, 1977, provides some insight on how a small dedicated group of Communists can disrupt vital processing and cause millions of dollars in damage.

These problems may be associated with Europe today; however, I fear that radical groups may attempt to hold either a major corporation or Government data center for political or monetary ransom.

Witnesses before this committee have identified a few of the radical groups and the thrust of their movements. Are we to let them, in the name of privacy, fair credit reporting, equal employment rights according to the newly defined handicapped, and so forth, allow these groups to operate without surveillance in our democratic society?

There may have been abuses on the part of law enforcement and other intelligence-gathering agencies in the past. However, today they are almost totally ineffective due to the operational and administrative constraints Federal, State, and local legislative bodies have placed upon them.

Imagine what the consequence might be if a radical group occupied the Social Security Administration's (SSA) computer center a few days before the monthly checks to millions of Americans were produced.

A threat to destroy the 30-odd computers located in the SSA main data center alone will create sufficient fear in the hearts of man, HEW officials, the legislature, and the American people that the Government would most likely negotiate.

The results, undoubtedly, would be a victory for the terrorists and a resounding defeat for our system of government.

Gentlemen, I have not appeared before you today with the thought of trying to reverse or otherwise overturn existing legislation. My purpose in speaking is to acquaint you with some of the problems we in the private sector and you in the Government must be ready, willing, and able to address now and in the future.

Life, liberty, and the pursuit of happiness are the concerns of all of us. However, we must have realistic and prudent measures by which we can collect and exchange meaningful and factual information about those individuals and groups that may intend to commit crimes and/or attempt to forcefully change our form of government against the will of the majority.

Thank you.

If I may, I would like to add a few items.

Mr. Short asked me if I had any documents I would like inserted in the record. I'll provide copies of those that I have with me and send you copies of those I have at home.

Mr. SCHULTZ. If you'll identify them, we'll ask that they be included in the record.

Mr. BAIRD. The first one is "Identifying Computer Vulnerability," a reprint from Data Management, June 1974.

An article entitled, "Auditing Around the Computer Center," appearing in Security Management, September 1976. This is the ASIS publication.

I will provide a copy of the Computerworld, August 29, 1977, article captioned, "DP Center Bombings Plague Italy."

I have provided Mr. Short with a résumé detailing my professional background. That may be used as the committee sees fit; however, I do request that my address be deleted from it if it is used.

That is all I have at this time, sir.

Mr. SCHULTZ. Those documents, pursuant to the order of the Chair, will be accepted for the record.

[The material referred to may be found in the files of the subcommittee.]

Mr. SCHULTZ. Mr. Baird, just one brief question before we turn to Mr. Larsen.

Is there no computer hardware available by which to preclude unauthorized access to computers?

Mr. BAIRD. No, sir. The technology is such today that we cannot insure the inviolability of the computing system. Perhaps in 8 to 10 years we may. The equipment manufacturers, I believe—I do hope—are addressing this problem.

Mr. Watson, then chairman of IBM—International Business Machine Co.—several years ago, announced publicly that IBM was going to spend multimillions of dollars on an investigation, review, and evaluation of computing systems security problems.

A report has been issued. I prefer not to comment on the content of it at this time. It is quite a large report.

Mr. SCHULTZ. I thank you.

Maybe we can hold this subject matter for the whole panel.

Mr. Larsen, if we might hear from you now.

TESTIMONY OF JAN F. LARSEN, MANAGER OF CORPORATE SECURITY,
PFIZER, INC., NEW YORK, N.Y.

Mr. LARSEN. I am honored to have this opportunity to appear before the Senate Subcommittee on Criminal Laws and Procedures to present this statement based on my experience on the erosion of law enforcement intelligence and its impact on public security.

I am employed by Pfizer, Inc., as manager of corporate security. Pfizer is an international, research-based company with 130 manufacturing and research locations in 21 States and 37 countries. Net sales are about \$2 billion.

Corporate divisions include Rorerig, Pharmaceuticals, Coty Cosmetics, Howmedica, Leeming/Pacquin, and Quigley.

As manager of corporate security, I am responsible for the company-wide conduct of internal and external investigations involving employees and others. It is my responsibility to manage these active investigations and, if necessary, evaluate the availability and reliability of private outside investigative services and direct and control their efforts.

My security functions do not differ in many ways from the investigative work of many law enforcement agencies, as they may involve theft, fraud, subversive activity, sabotage, and other activities detrimental to the company.

I also have to maintain an effective liaison with my company's legal, personnel, public relations, labor relations, and other divisions.

In addition, I have to maintain a strong liaison with all levels of law enforcement in order to do my job effectively.

One basic responsibility of the security organization of any company is to conduct investigations involving a loss of company assets. The basic premise on which security investigations are conducted is that the investigation be completely unbiased. The reputation of employees is very important; therefore, allegations are disproved as well as proved.

Any cutdown on the effectiveness of law enforcement hurts everyone. There is a definite need for intelligence agencies to exchange and coordinate information regarding various criminal activities. Much of this information can prove invaluable to industry if properly used.

In the areas of personnel records and reviews of criminal background checks, there is a strong desire to eliminate applicants with poor reputations and undesirable backgrounds. Keeping such people out of our organizations may prevent many future security problems.

Law enforcement agencies are highly conscious of the adverse effects a criminal history can have on the life of an individual who wishes to avoid future criminal involvement. Corporate personnel organizations are equally concerned of the confidentiality of an employee's personnel record.

Years ago, it was a routine matter for personnel departments or security organizations to conduct criminal background checks on prospective new employees. Criminal checks for new employees are

no longer required by Pfizer—nor are they available. Applicants are screened by personnel on the basis of the applicant's own records, references, and the personnel interview.

During a 3-year period, I personally cannot recall an instance where a criminal background check for a new employee was necessary, except in cases where a Department of Defense clearance is necessary—in which case these employees are investigated by the U.S. Government.

I believe we have been fortunate in our selection of personnel.

However, industry can benefit from receiving certain law enforcement intelligence information. Information on terrorists, radical groups, organized crime, and receivers of stolen property, all of which may affect the company's operation, is extremely important information to evaluate in order that the company can put up an adequate defense.

Intelligence information on organized crime could prove invaluable to many companies located in areas which are targets of organized crime.

Gambling on company premises is of great concern to corporations. Gambling has been with us as far back as anyone can remember and certainly is with us today in all forms. Security organizations are realistic in thinking that gambling will never be eliminated, but we do try to minimize it.

Gambling creates potential inroads to various company locations by organized crime. Many large plants are made to order for large-scale gambling operations of the type controlled by the well-organized criminal element.

As with drug pushers, members of organized crime will take advantage of a workingman in an industrial climate, certain that he is not an undercover law enforcement agent.

Almost without exception, where there is widespread gambling, there are loan sharks. When these elements are together and organized, this can result in dishonesty among employees under pressure to meet gambling losses and other indebtedness.

Organized crime attempts to worm its way into industry in many ways. Today large corporations are diversified and acquisitions of new companies take place quite frequently. Before an acquisition or merger, a corporation must be convinced that the company has no ties to organized crime.

Law enforcement should be permitted and encouraged to assist corporations with the available intelligence information on a routine basis if an inquiry of this nature were to be made.

Almost every major firm in the United States has increased its security in the past years, including plant protection guards as well as trained security investigators. Many new housing developments and shopping centers have their own private or contract security force. Security personnel at airports have more than doubled. Purchasing of security hardware, cameras, alarms, et cetera, as well as increased use of fancy motion detection equipment, et cetera, has also increased.

This focus on increased private security is going on in spite of the fact that every major law enforcement agency has added to its personnel, and most areas of law enforcement have received aid from the Law Enforcement Assistance Administration.

Increased security protection is brought about mainly by management acutely aware of the increase in crime. There is also a growing fear of personal safety, especially among executives who have high visibility, while representing their corporations.

The media has also been a factor in the increase of security protection by letting the public know that existing law enforcement organizations are inefficient in coping with terrorists and criminal elements.

In today's climate when there is a general lack of confidence in the criminal justice system in dealing with criminals, it seems that protection rather than prosecution is the surest solution. Much of this can be avoided by effective law enforcement cooperation.

Thank you.

Mr. SCHULTZ. Thank you, Mr. Larsen.

Your prepared statements have a central theme.

One, as corporate security officers you are vitally concerned with the protection of assets and revenues; and that you rely upon information to make management decisions by which to protect these assets and revenues.

The subcommittee has received testimony and evidence clearly showing that there is today an erosion of the law enforcement capability to gather intelligence.

Gentlemen, the law enforcement community gathers intelligence from people such as you who are policy setters and who have an input into the way a company is managed.

Tell us, if you will, have you been precluded from cooperating with the law enforcement agencies?

I don't mean to put you on the spot, but it is a two-way street. You would like information and you would like help. Are you able to provide information freely to the law enforcement people?

Who would like to start out? This is a panel question for all of you. Mr. Duckworth?

Mr. DUCKWORTH. Mr. Schultz, the decision on whether or not to release information in our company--especially regarding individuals--is basically a discretionary decision. It's made by our personnel manager, or someone within the personnel department.

That discretionary decision generally is based upon the nature, purpose, and a subjective evaluation of the legitimacy of the request.

If the response does not seem to meet this subjective criteria established by the personnel manager, then the request would be turned down; and he would require the information to be subpoenaed or obtained by other legal action.

That has happened, and we have complied, obviously, with the subpoena.

If it seems that, based again on this admittedly subjective evaluation, the request is legitimate, the information will be provided.

This must be caveated, I think, with the point that the information that's released is also subject to his discretionary review. The agency making the request, if it's legitimate, may or may not get what they are actually looking for.

I think that this illustrates a point that is extremely important and crucial to this subcommittee. There is a sense of caution which pervades both industry and the law enforcement intelligence organizations or law enforcement today. I think that that sense of caution is basically as a result of the existing privacy legislation.

In industry, perhaps it is not a direct result. However, the confusion factor that has resulted within the public sector as a result of the privacy legislation has caused this sense of caution on behalf of industry.

I believe in many cases it has practically turned normal relationships into a mere paralysis of effort or interface between the law enforcement agency and industry.

Mr. SCHULTZ. Are you saying that the same policy applies between companies, as between company and law enforcement officials and agencies?

Mr. DUCKWORTH. For the most part, I would say that it does.

I think that the majority of companies are extremely hesitant to reveal any more than the minimum they think they can get by with another company.

Mr. SCHULTZ. Mr. Baird, you had a comment?

Mr. BAIRD. Mr. Schultz, I'd like to amplify Mr. Duckworth's comments that pertain to information flow between companies.

As an independent consultant, I get around and visit quite a few different companies during the course of my business.

I find a very severe reluctance on the part of the corporate personnel managers to make available to another company adverse information about an employee that has committed some form of criminal act within that company.

The rule--the unwritten rule--seems to be that companies will only divulge the date of employment, the job title or position, and the date of separation, and often nothing more.

A few companies I have been in would make an additional statement as to whether or not the employee is rehirable--and no more.

Most criminal activity in my area of specialization--data processing--based on that 1973 study, indicates that as many as 85 percent of the subjects were not brought before a bar of justice.

That being the case, there are no criminal records.

Industry's reluctance to report computer crimes is also a part of this problem.

Currently before the Senate is Senate bill 1766, which is entitled: "Federal Computer System Protection Act of 1977."

This bill is a giant step forward in providing legislation applying criminal sanctions against computer criminals. However, the law, in my judgment, does not go far enough.

The State of Florida has formed a special investigative unit. I believe it's titled "The Strategic Investigations Unit."

Illinois has their specialized crime-fighting unit. And the FBI has entered into the computer crime area with a training program which was recently announced and shown on the NBC News broadcast this past Monday evening.

These are three agencies that are now looking into the problems associated with computer crime.

However, there was some talk not very long ago that the Florida unit might be disbanded or have its computer crime function taken away from it, because it was not receiving any reports of crime.

In my judgment, the legislation before the Senate needs to be amended to apply the same criminal sanctions against the management of a corporation and/or its data processing manager for the

failure to report to the proper authorities criminal activity of some magnitude.

We have a long way to go.

Mr. SCHULTZ. In other words, you're saying that there should be a mandatory requirement to report a crime, once determined.

Mr. BAIRD. Yes, sir. I believe that the vehicle is the Senate bill 1766. It applies to many—it makes it a criminal offense to abuse computing systems that are engaged in interstate commerce or covered by Federal legislation, such as the Banking Act, defense contractors, and things of that nature. It covers a wide multitude of systems.

But, yes, I think that the legislation should require and make it a penalty not to report these crimes.

The stockholders of companies, for example, are the losers, as is the consuming public. We pay for these crimes in the form of a tax—a rather hideous tax, called increased price of goods and services.

The stockholders are cheated out of, perhaps, additional earnings that should be distributed to them.

We're paying a very heavy tax for crime—not just in the data processing area, but throughout all the industries represented here and that are represented by the American Society for Industrial Security.

That covers the whole ball park.

Mr. SCHULTZ. Your recommendation will, of course, be noted in the record.

I am aware of S. 1766, though I am not intimately familiar with all the provisions.

Congress is, and has been, careful to not unnecessarily legislate in the area of private enterprise. To make it a crime to fail to report a violation of computers—it's worth exploring. I'm not sure how you would enforce that. That would be one of the problems.

At what point do you determine an entry has been made in the computer?

I don't want to get into this, because I'm not an expert in computers.

But is there another comment? Mr. Duckworth?

Mr. DUCKWORTH. I would like to say, from industry's perspective, that I think we would concur with your comments, Mr. Schultz. I think it would be very difficult, for the most part, for us to ascertain in these cases that perhaps a crime had occurred.

I think that what you might find is overlegislation in this field, which perhaps could be handled by some of the large companies. But I'm not too sure if any small company would be able to comply with that recommendation.

Mr. SCHULTZ. In any event, Mr. Baird, you are supportive of S. 1766?

Mr. BAIRD. Yes, sir; my support is there.

Mr. SCHULTZ. Mr. Larsen?

Mr. LARSEN. I feel that it is not a deterrent to crime if an employee is apprehended in a criminal act and he knows that his criminal history will not follow him. This knowledge should give him a secure feeling and possibly an incentive to continue in his area of crime to know that if and whenever he is apprehended his crime will remain a secret. I have my own thoughts on the cataloging and retention of criminal records. Depending upon the seriousness of the crime, records should be made available and retained for certain periods of time.

Serious crimes should remain on record for a longer length of time and minor offenses should remain on records for only brief periods of time. Repeat offenders or offenders of various crimes would have their records available for longer periods.

Mr. SCHULTZ. Is there any other comment? Mr. Ruane?

Mr. RUANE. I would like to say in the personal area, to include security, that there are many portions that we have to contribute to—not only as an employer but as a security force within corporate.

The question was asked: Do we interchange information with law enforcement agencies?

In most cases, when I conduct an investigation and bring that investigation to a successful conclusion through litigation, and the finding is on behalf of the corporation and against the defendant, we disseminate that information as to the amount of revenues obtained by that defendant through illicit trafficking. We return that information over to the Internal Revenue Service for their evaluation and possible prosecution.

Mr. SCHULTZ. Thank you.

The subcommittee has received information and testimony that, in fact, the law enforcement people—not as a general rule but in certain areas—have become reluctant to record the general intelligence information that they obtain in their day-to-day activities. By recording it, I mean to reduce it to writing and memorandums and to file it.

Of course, this makes for an even more dangerous area, because they are working out of their hip pocket—what they remember. And when they pass it on, the information might become distorted.

My question to you is: As corporate security officers, if you were provided with raw intelligence data, do you have the capability to analyze it, to use it, or to hold it in such a manner that it is intelligence and not something that would get out and hurt private individuals or employees of your own company? Could you handle it? That's the basic question. What would you do with it?

Mr. DUCKWORTH. My understanding of intelligence is that it is processed information that has already gone through an intelligence cycle in which that information has been analyzed and rated in terms of its accuracy and credibility. The source has been identified and also given some form of rating.

What I'm indicating is that intelligence, as I understand it, is refined data or refined information. And that's one type of information that I think I would be looking for—information that has already gone through the intelligence cycle and is provided to us.

Raw data I don't think I could use—and I don't think that I really want it. I would be quite concerned about any type of activity which would simply pass me raw data.

Mr. SCHULTZ. I submit there are different kinds of intelligence information. One example—a man has been convicted of bank robbery twice and has done 10 years in prison—as opposed to an officer coming to you and saying, we have information that an individual was a member of the Weather Underground and that he participated in three bombings and he now works for you.

I am distinguishing between raw intelligence data as it relates to your need to know, and how you would handle it and whether you are equipped to handle it.

It would be nice if you had documented testimony and a conviction record all in a nice, neat package. That's not too hard to handle.

I'm talking about the difficult one, where it is in fact raw intelligence data—perhaps unsubstantiated.

Mr. ENGLISCH. I might suggest that what has happened in this connection is that the recipient of informal information of the nature that you describe, as opposed to a specific report and a signed intelligence document authorized and certified by an agency, has become a situation very few people would ask for—for the simple reason that it is not going to be given to them on an informal basis.

If it is given to them informally, there will be an informal personal comment: "You've got it; that's it; don't come back to me about it" sort of response.

It has developed between industry and law enforcement and between industry itself of a general reluctance to even look for this information for the simple fear of placing yourself or your company in a liable position.

An individual can see, as can the company, the costs and time involved in this type of pursuit are totally unacceptable to an industry today.

As a result, you find that personnel officers and security officers will refrain from even attempting to obtain information on that basis, for the simple reason that they cannot use it.

We've reached the point that many of our personnel and security people have stopped asking for it.

Employee applications and the information you get from the employee himself—what can you gain from that today? I assume that it is very little.

I'm sure you're aware that you are no longer allowed to ask a person's age, marital status, or anything like that. The closest I've seen to being specific is an entry saying: Are you under 18 or over 40?

In a situation like this, you look back and say: Have we been damaged by not having been able to get this information?

In most cases, you will find that you can't say: Yes; this level of crime has occurred in my company since we stopped doing this. It is very hard to pinpoint.

I do say it is a sleeping giant of great proportions.

The pervasive effect of the ability to get into a company because that information is not available is a precursor to problems of the future.

The unfortunate fact is that not enough significant incidents have occurred that can be traced to the shortage of intelligence information.

The security and personnel people are being deluded into a sense that everything is fine.

I'd like to use a very trite observation here. It is just like saying: Why install fire alarms, because we haven't had a fire recently.

We're in that position. It's not there; it's not being offered. We've reached the point where we're going to ask for it.

I think this is detrimental to the public interest.

Mr. SCHULTZ. You bring up a very important point.

Of course, though we are thankful for the absence of any great catastrophe which would require a management decision based on intelligence or security which we don't have, the problem is, Should that occur we probably would be required to shoot from the hip to come up with an answer to cope with it.

That is basically what we are concerned with here today in this hearing.

Mr. Martin, did you have some questions which you wanted to ask?

Mr. DUCKWORTH. May I return to your original example for a minute?

Mr. SCHULTZ. Yes.

Mr. DUCKWORTH. I would like to use that example to perhaps take you through a scenario in which you might find a security officer working.

The first part of the example that you used—an individual having an arrest record with convictions—is generally available to us today, especially in most jurisdictions. I think that we have no problems in handling that. That is fairly self-explanatory.

In your second example, I also agree with you that there is certainly a difference in types of information but submit that it is equally important, if not more important, for us to have knowledge of the individual cited in the latter example.

Perhaps it's a matter of semantics and our having trouble defining exactly what we talk about in terms of intelligence.

To go back to my days in intelligence operations, in Army intelligence particularly, we evaluated both the source and the information.

I see that the latter example, to me, falls into that type of category in which the intelligence unit would provide an evaluation of the source as well as an evaluation of the information.

I also see that the benefit then that the security function derives from having that information is that you can then begin to more accurately assess the threat as well as develop effective countermeasures.

In addition to that, you have the potential at that point in time for deciding that if you want to pursue additional preventive measures or additional security measures on your own, for example, you might initiate a more in-depth investigation using your own resources.

It might—take the form of a truth verification device or it might take the form of some type of so-called honesty test.

And even if you chose not to use one of these alternatives, you would still have the knowledge that you have a potential threat; and then you could possibly develop more conventional countermeasures in a particular area.

You might refrain from assigning that person, for example, to a position in which he might have unrestricted access to certain types of assets where the potential for loss is great.

Given the set of circumstances postulated in the Weather Underground example, there are an infinite number of security precautions which could be taken based upon that information without infringing upon the individual's personal rights. Without that information, the options that you have become quickly limited.

I do not advocate unlimited passing of raw information without some constraints nor do I condone or accept the "right" of a terrorist organization to bomb or otherwise destroy my company's property.

It seems to me that the question is not one of our basic need for this type of information or even our societal "right" if you prefer, but rather the form of the information transfer and the safeguards and precautions associated with this transfer.

Mr. SCHULTZ. I would have to conclude, though, that you would resolve all doubt in favor of your company.

Mr. DUCKWORTH. Absolutely.

Mr. BAIRD. I'd like to add a comment to Mr. Duckworth's remarks.

He made mention to truth verification techniques that are currently available to industry as well as government.

One of the recommendations of the President's Privacy Protection Study Commission is that the Congress outlaw any and all use of truth verification techniques as a violation of an individual's privacy.

In this case, as described by Mr. Duckworth, we are trying to verify the truth of a condition by whatever techniques technology has given us today.

I'm afraid that this will be further erosion of industry's ability, as well as Government's ability, to protect its assets.

Mr. SCHULTZ. Thank you, Mr. Baird.

Mr. MARTIN, did you have some questions?

Mr. MARTIN. Yes. I have a question for Mr. Englisch first and then some questions for the panel.

Mr. ENGLISCH, you provided the subcommittee with a chart which indicated that there had been a good deal more cargo theft as a percentage of total cargo loss in recent years than there was, let us say, 10 or 15 years ago.

Mr. ENGLISCH. Yes.

Mr. MARTIN. I don't happen to have the chart in front of me, but I think it starts with the year 1973 or 1974.

It starts with 1973.

Mr. ENGLISCH. Yes.

Our chart reveals that they are in 5-year groupings of statistics which represent the loss that we could categorize as theft, reported by our insureds in the cargo area.

These are policies covering the cargo.

There has been a significant increase, starting in the years 1951 through 1955, of 24 percent estimated, through the year group 1969 through 1973 of 33 percent.

We are presently gathering statistics for the next edition which should appear in mid-1978. Trends right now indicate that that 33 percent will be substantiated—if not increased slightly.

You must recognize, however, that these statistics are based on reportable losses; losses reported by our insureds.

As a cargo policy will have it, they are tailored to each individual insured having different deductibles, for example.

Quite frequently, we'll have a major company making shipments with a deductible of \$50,000 for any one loss. This means that any loss under that is paid from that client's operating expenses. It is not reflected in our statistics.

So, again, we may be showing you the upper portion of an iceberg in this case.

I'm sure you're familiar with the program against cargo theft, which initially began in 15 selected cities in the United States, of a group operation between law enforcement agencies and private industries and the Department of Justice. Later it was transferred to the Department of Transportation.

In this area, we have been attempting to work on a cooperative basis in these various cities where cargo theft was identified as a problem.

The results have been spotty. In some places, there has been improvement in communication and exchange of information. But primarily information so that you could take efforts of a positive nature—increased physical security and fencing and lighting and so forth—has improved the situation somewhat.

But really the area of the collusive effort between people who are designing an effort to remove cargo from its normal track continues, in my opinion, quite unabated. It is a significant problem.

I might address an additional remark, if I may, which relates to a subject matter Mr. Duckworth just pointed out. That is, the action you take within your own company in receiving informal information on a particular employee.

One of the suggestions is that you might restrict that person to a particular type of work where this issue would not create further problems.

If you do this, you must do it in full knowledge of the present requirements of the affirmative action program, recognizing the person's career path will be tested by audit from time to time to determine if there is any discrimination against this particular employee.

Unless substantiated by specific criminal records, it is going to be very difficult to preclude a citation against your company in that area.

Again, here is another area which impacts the decision of the security executive of the company in his approach to solving the problem.

The end result appears to be a greater dollar investment in hardware to attempt to preclude this type of crime, as opposed to removal of the threat source.

In other words, you build a wall.

Mr. SUORT. You almost have to have a conviction then before you actually can act?

Mr. ENGLISCHI. I would say, yes.

Mr. MARTIN. Suppose an employee is caught in the act of pilfering. He's arrested and indicted. At that point could you provide such information to another company if he applied for employment in another company?

Mr. ENGLISCHI. Not until a conviction was obtained. We would say that the individual left our employment.

We could not say that the man is guilty of anything until he is found so guilty. In so doing, I open my company up to a state of being liable for our actions.

Now he may be discharged, and he may accept this discharge or he may not. If he is discharged in the cargo area, quite frequently, the next day, he'll be working for another company because he is replaced by other private employment means. He may go through a local or whatever he works for.

But he may find himself an indicted person for a year or more before his case comes to trial and working in an area where there is similar access to cargo.

Mr. MARTIN. Neither his previous employer nor the law enforcement agency can provide this information about his arrest and indictment to his new employer?

Mr. ENGLISCHI. I have not personally been in a situation very recently to have to have asked that question. But I must admit that it would be a very interesting question to ask if I could get an affirmative answer.

Mr. BAIRD. May I add to that, Mr. Martin?

There are two recent experiences that I've had with clients:

In one instance, a young man attempted to sell his company's customer name and address list to competitors. He was asking \$2 per name and there were in excess of 297,000 names on the list.

He was apprehended and indicted; however, the personnel policies of his former employer were to only confirm dates of employment, job title, scope of work, and date of termination.

I was physically present in the personnel manager's office when a call was received from a prospective employer. That's all that would be verified.

I asked why wasn't the caller advised that this individual was not subject to rehire or that he was currently indicted.

The second instance I'd like to bring to your attention is another area in which a superior—

Mr. SHORT. Excuse me. Before you go on, what was the response to that? Why didn't he say that he was indicted? That's public information.

Mr. BAIRD. It's public information; it's corporate policy; and they did not want to become involved.

In this instance, what we're doing is just passing on from one employer to another unsuspecting employer an individual who has certainly demonstrated by his actions some question as to his trustworthiness.

In the second incident, an accounts receivable supervisor manipulated the data processing environment for personal gain. It wasn't very much—\$3,000.

After the event was discovered, by accident, the employee was discharged. Later on the employer found that this employee had three arrests warrants outstanding—one for prostitution, and perhaps drug involvement; and another one for fraud; and I don't recall what the third was.

The point I wish to make is that this was only discovered after the employee had taken this company for several thousand dollars.

There is a pressing need for information, gentlemen. It is just not readily available. The climate today is such that companies are very reluctant to ask questions.

Mr. ENGLISCH. May I offer a simple hypothetical case in which an employee is found leaving the compound with cargo.

Let's assume it's a managerial person. The state of affairs at that point in time is that he resigns.

A few days later you get a request as to the background of this employee, because he's looking for another job and has applied with a different company.

You are in the position now, having discharged the person or having him resign of his own volition, that he has left. Now what can you tell the prospective employer?

Let's presume you say you asked him to resign because he stole cargo. You are now placing yourself in the position where that employee, if he loses the job he's applying for because of your statements, it is not unbelievable that he would take legal action against your company.

That's what happened.

Mr. MARTIN. Could you move the microphone a little bit closer to you, sir. We're having trouble hearing you.

I have just a few more questions. It is pretty late. We will try to wind up as rapidly as possible.

You have all made the point that industry and business are encountering increased security difficulties as a result of the privacy legislation and the erosion of law enforcement intelligence.

You have told us, as a result of this, you have had to vastly increase expenditures for security purposes, piling on more security hardware and substantially increasing your security personnel.

Would you be willing to venture an estimate, based on your own experiences and what you've heard from other people in the security field, of the increase in expenditures for security purposes by corporations over, say, the past 5 years?

Mr. BATRD. I'd like to respond to your question.

One, I think it's impossible to develop a comprehensive dollar value or percentage increase in those costs.

Within the last year or two, I do not recall my source, the security industry was rated as one of the three top growth industries in our Nation.

I believe that will give you some feel for the magnitude of this problem.

Mr. SHORT. I heard today on the news that there are as many private security officers in the United States as there are police or law enforcement officers today.

Mr. RUANE. In the hardware area, on Long Island, there are about 25 known companies who deal in electronic surveillance equipment, whether it be U.S. manufactured or in other countries such as Germany and Japan.

These companies have grown from about a \$60,000 company—the one that I'm thinking of specifically has grown from a \$60,000 company to a \$7.5 million company within a period of about 3½ years.

That's just one company.

Mr. ENGLISCHI. I might also interject, although it doesn't relate to hardware, our own society—the American Society for Industrial Security—has essentially doubled its membership in the past 5 years. It has gone to 10,000.

This, I think, is a very good bellwether of corporate interest in the security area.

Mr. MARTIN. In short, if you can judge from your own membership, the number of security personnel throughout the Nation has probably doubled over the past 5 years.

Mr. ENGLISCHI. Yes.

Mr. DUCKWORTH. I would say that I would also like to cite a report by Frost and Sullivan, a research firm located in New York, which made a comprehensive study of the entire security market. That consists of hardware, software, personnel, alarm systems, and the whole spectrum that we talk about when we talk about countermeasures. I don't have the specifics, but it also could tell you that it was one of the fastest-growing industries in the United States. By 1981, if my memory serves me correctly, the total market would have tripled in size.

So I would suggest that the Frost and Sullivan report—or a summary—could be included in the record, if the record can remain open until I can forward you a summary of that report.

Mr. MARTIN. If you can provide us with a copy of the report, I think it might be useful to include the summary in the record, or in the appendix to the record.

[The material referred to will be found in the appendix, p. 131.]

Mr. MARTIN. I'd like to ask this question:

If we keep on adding to our security hardware every year—adding security guards at every industry and every place of business—isn't there a danger that as a result of this exaggerated regard for privacy, it will ultimately transform our country into a garrison society?

Mr. BAIRD. I'd like to answer that, Mr. Martin.

I think we're pretty close to being there right now.

Industry is very much concerned and so is the individual citizen.

I, for example, have had my home burglarized twice. I personally have had to go out and spend approximately \$1,200 to put in an alarm system to protect my home and property.

The elderly in many of our cities live in great fear. They are attacked, robbed and beaten on the streets and even in their homes. It is not uncommon for senior citizens to equip their homes with all sorts of locks and devices to keep intruders out. Unfortunately, these fortresses are in fact their prisons.

Industry is also expending large sums on guard forces, fences, locks, alarms, et cetera, in their attempts to protect their property.

Yes; I think that we are rapidly approaching a garrison environment.

Mr. ENGLISCHI. I would emphasize this by suggesting that if you ever have the opportunity to sit with the truck drivers approaching a terminal in the Port of New York area, you will find that he is stopped at the gate, his cargo compartment is searched, the front compartment is searched, and he is driven to a special holding area that is constructed just for holding incoming truckers.

He debarks from his truck and he and his documentation are photographed. He is then put into a waiting room until his truck is called to pick up its cargo.

He picks up the cargo. He gets a cross-signature check of three separate signatures for the cargo he's about to leave with. As he approaches the gate on departure, his truck is again opened and inspected to see that it has the cargo that is on the bill of lading he carries. The driver's compartment is again searched. And only then is he allowed to depart the terminal.

I submit that if that's not a garrison, I don't know what one is.

Mr. RUANE. The systems have been compromised, and that's why we're here.

With all of that expertise and providing the security methods at hand, we know that the systems have been compromised to the tune of about \$1 billion a year in transportation. So we really come back to a people problem that has escalated in the last 20 years I'd say. People have not been able to distinguish a moral code that has eroded to a situation that must necessarily force industry to make a garrison society.

Mr. MARTIN. I want to be sure I understand what you're driving at.

Are you saying that additional hardware is not a substitute—an adequate substitute—for a good personnel security program supplied with adequate information?

Mr. RUANE. That is correct.

Mr. ENGLISCHI. Just because this garrison I've just described exists, it doesn't mean that the cargoes are still not stolen.

We may recognize that the driver approached the terminal with an original bill of lading that was obtained by bribe and through his co-conspirators he has timed his arrival to beat the actual pickup truck and makes the ripoff, so to speak, in that fashion.

Again, it is in periphery industries as well. It is not just the transportation industry itself.

Mr. BAIRD. I'd like to state, gentlemen, that we have fundamental problems—I think an attitudinal problem—on the part of our society, or at least many members of our society.

I have here, once again my favorite source, the U.S. News & World Report of April 28, 1976, an article, entitled: "Ten Days to Rip Off Society."

This news magazine surveyed a number of newspapers in some 16 cities during a 10-day period.

It is reporting on fraudulent and illegal activities on the part of citizens, many of which we were taught by our parents to respect and admire—doctors, lawyers, politicians, and appointed officials.

I will include this article with my material.

What I'm trying to point out is that we have an attitude problem in our country where ripping off the system is almost an accepted way of life today.

This attitude creeps throughout our society.

We also have a mobility factor. Transportation is a mobile item. Commodities are moved by truck. But people move also. We have a great deal of human mobility in our society. This mobility and the existing restrictions on the exchange of information presents a situation in which both law enforcement agencies and employers are almost totally unaware of an individual's criminal background. This is especially true when people move from one State to another.

Mr. MARTIN. I would like to amplify the question with an additional question.

When you create a situation that makes it easier for people to rip off society, doesn't this, in effect, encourage them to rip off society?

Mr. BAIRD. Yes, sir. Very definitely.

Once again, I would just like to talk about the data processing area.

There are very bright technicians that work in this area, and they don't view manipulating computers and the assets stored in them as being a criminal act.

Quite often they view it as: I'm not hurting anybody. It's only the company or government and they would never miss the little that I take.

So this does increase this problem wherever you go.

The unfortunate thing about society is that there is no such thing as swift and just punishment—or very little of it.

Mr. LARSEN. I would like to refer to an earlier comment regarding increased security. It appears as a bit of irony that many companies have facilities and warehouses that have millions of dollars worth of inventory and raw materials that must be protected. Thousands of dollars are spent on security hardware and then the company relies on the protection, alertness, and honesty of a contract guard who may receive less than \$3 an hour. This guard may be an individual in which the guard agencies themselves have not been able to do a background security clearance. Many companies are faced with the problem of having to put security on security.

Mr. RUANE. It is actually a fact that 3 weeks ago in the State of Illinois, where we have a branch operation, one of the security officers on duty on a weekend went to his car on five occasions and had about \$1,000 worth of jewelry in the back of his car when we made the apprehension of him. The total loss over a 10-week period by this guard was in excess of \$60,000.

It can't be emphasized enough—and Mr. Short said—that there are more private security officers in the United States, or as many, as the legitimate law enforcement agents in the United States.

So they are a viable force that has to be dealt with. And the industry has to deal with it insofar as having intelligence to let them make the proper decision as to where and how and why an individual can be put into a position of trust for the protection of industry on the whole.

Mr. DUCKWORTH. We can perhaps reduce this to simplistics. We earlier mentioned a garrison society, and a ripoff society. Without a doubt, and we all agree, that's what we have today. Who suffers in the corporation? We all do.

The thing you have to understand from our point of view, and the point of view of any business, is the fact that not only do we represent the formal structure of employees and management but in effect we represent all the shareholders and indirectly the consumer.

When we talk about crime affecting the corporation, we are talking about the fabric of our society, and we are all affected—from employee, to shareholder, to consumer.

The title of the hearing on the letter I got was the "Erosion of Law Enforcement Intelligence and Its Impact on the Public Security."

I thought that was extremely apropos because our various organizations are the public.

To me, the crux of the argument is that we need the information that, if nothing else, provides us with the knowledge of a clear and immediate danger—as I characterize it—that something is going to happen in the organization; that crime is going to affect it in any of its myriad forms.

That is crucial to our success and, consequently, crucial to the success of our companies and to the public sector.

Mr. SHORT. You stated in your opening remarks, Mr. Duckworth, a concern, and I quote:

That law enforcement intelligence capabilities have been weakened to the point where they can no longer even warn me of a clear and immediate threat which places corporate assets and people in immediate jeopardy.

So if this happens, then you are completely out of business.

Mr. DUCKWORTH. Absolutely.

Mr. ENGLISCH. If it would interest the subcommittee, I might commend a short film that was made by CBS, I believe, as part of their "60 Minutes" program in early 1962.

The title of the 20-minute segment of the program is called "Thievery on the Waterfront."

In that film, one of the people who testified before this subcommittee was interviewed in the film and made some comments.

I would just like to offer the observation made by Mr. Louis Tyska, who at the time was a private security man who subsequently became director of cargo security for the U.S. Customs Office.

He said:

We are competing with a business--

Addressing the thievery business on the waterfront—

that is very difficult to compete with because it has a very low overhead.

I submit that the magnitude of crimes and the magnitude of organized effort to broach the transportation system in cargo crime may be without parallel.

Mr. MARTIN. I have one quick question I'd like to ask in the form of a summary.

I want to make sure that we understand what has been testified to today.

It seems to me from your testimony that there exists a four-way freeze on the exchange of intelligence.

First, private business concerns are fearful of divulging information about employees and clients to law enforcement agencies; and they don't do so ordinarily unless they are confronted with a court order.

Second, one industry cannot provide information about a former employee to another industry, even where the employee in question has been dismissed for theft and indicted.

Third, private industry cannot do a background check of any kind with law enforcement agencies, even in the case of applicants for sensitive positions, unless they are working on defense contracts.

And fourth, our law enforcement agencies themselves frequently don't have any information because of the near freeze on the exchange of information between Federal, State, and local agencies.

Would you say that's an accurate summary of what we've been told?

Mr. ENGLSCII. I'd agree with that.

Mr. DUCKWORTH. Yes, sir.

Mr. BAIRD. Yes.

Mr. SCHULTZ. Gentlemen, we thank you for your testimony, individually and collectively. And a special word of thanks to you, Mr. Duckworth, for your efforts in putting the panel together under the auspices of the American Society for Industrial Security.

We will continue our hearings and look forward to concluding them perhaps early next year in connection with the erosion of law enforcement intelligence-gathering capabilities.

We did not intend to put corporate security under the spotlight today, but we do appreciate your willingness to come in and testify and let us understand what some of your problems are in dealing with crime and intelligence-gathering generally.

The Congress does not legislate in a vacuum. They do need to know what your problems and your interests and your needs are.

For assisting in our inquiry we thank you.

We'll stand adjourned, subject to the call of the Chair.

[Whereupon, at 1:30 p.m., the hearing was adjourned, subject to the call of the Chair.]

APPENDIX

(From Private Security, "Report of the Task Force on Private Security, National Advisory Committee on Criminal Justice Standards and Goals, Law Enforcement Assistance Administration.)

SECTION 6.—THE HISTORY AND DEVELOPMENT OF PRIVATE SECURITY IN THE UNITED STATES

Although the greatest growth in the private security industry has occurred in recent years, a review and understanding of the historical aspects that led to this growth are important. Through the review of the history, the present day state of the industry can be better understood.

EARLY HISTORY

The concepts and security practices that form the basis for modern American security can be traced to early England.¹ Colonists settling in a new and alien land banded together under a system of mutual protection and accountability that stemmed from early Anglo-Saxon times.² Prior to American independence, protection of the colonists and their property was the responsibility of town constables and sheriffs, supplemented in many towns, in English tradition, with watchmen who would patrol the streets at night. These watchmen remained familiar figures and constituted the primary security measure until the establishment of full-time police forces in the mid-1800s.

To ensure adequate protection, most local governments formalized the watch system and required each adult male inhabitant to serve a period of time as a watchman. A watchman's tour of duty usually began at 9 or 10 o'clock in the evening and ended at sunrise. During their tours of duty, the watchmen often encountered fires, Indian attacks, wild animals, runaway slaves, thieves, and grave robbers. They were expected to cope with these incidents and maintain order by quelling disturbances, arresting drunks, and enforcing the curfew. The watchman's job became increasingly difficult as industrialization and urbanization spread. Without training or legal support, and with little or no pay, most of those chosen to stand duty as watchmen would hire others to perform this unpleasant, thankless task. And, although the task of protecting their communities had become more difficult and demanding, watchmen were vilified and downgraded in the eyes of their fellow colonists.³

As security problems kept pace with the rapid growth of the country, public pressure mounted for increased and more effective protection. Attempts were made to add daytime complements to support and supplement the night watchmen, but it soon became apparent that the watch system was neither adequate nor efficient. This realization led to the formation of public police departments with fulltime, paid personnel. The first public police force in the United States was established in 1844 in New York City, and by 1856 police departments had been set up in Detroit, Cincinnati, Chicago, San Francisco, Los Angeles, Philadelphia, and Dallas. Although these early police departments were generally inefficient and often corrupt, and their personnel poorly trained, they represented

¹ Green, G., and R. C. Farber, "Introduction to Security," Los Angeles, Calif.: Security World Publishing Co., 1975, p. 23.

² Ursle, H. S., and L. E. Pagano, "Security Management Systems," Springfield, Ill.: Charles C. Thomas, 1974, p. 12.

³ Peel, J. D. "The Story of Private Security," Springfield, Ill.: Charles C. Thomas, 1971, p. 16.

a vast improvement over the old watchmen system. The Civil Service Act of 1883 was instrumental in rectifying many problems of the early police departments.

The emergence of public police departments, however, did not mean the end of private citizen involvement in the protection of life and property. Public law enforcement agencies were in their most incipient stage and could not keep pace with the mounting problems of crime in their communities. The incidence of crimes against property had become acute. The coupling of these facts forced industrial and business organizations to recognize the need for some form of effective security to protect their assets. Thus, in the 1850's major components of the private security industry were developed in answer to this need.

Allan Pinkerton formed the North West Police Agency in 1855 to provide protection for six midwestern railroads, and the Pinkerton Protection Patrol in 1857 to provide a private watchman service.⁴ For more than 50 years, Pinkerton's was the only company in the country engaged in interstate activities, such as the provision of security for many of the railroads. Pinkerton's also provided security for industrial concerns and was even hired as an intelligence-gathering unit for the Union Army during the Civil War. Today, Pinkerton's, with numerous services and activities, is the largest security organization in the world.

In 1858, Edwin Holmes began the first central office burglar alarm operation, which evolved into Holmes Protection, Inc. When the American District Telegraph Company (ADT) was formed in 1874, use of alarms and detection devices spread to provide protective services through the use of messengers and telegraph lines. By 1880, the use of electric protection for industrial and commercial enterprises in New York City was well established.

In 1859, Washington Perry Brink formed his truck and package delivery service in Chicago. He transported his first payroll in 1891, thereby initiating armored car and courier service. By 1900, Brink had acquired a fleet of 85 wagons. Seventy-five years later his security business was grossing more than \$50 million in revenue each year.⁵

During the 1800s, with the westward expansion of the United States, railroad lines moved into sparsely settled territories that had little or no public law enforcement. Trains were subject to attack by Indians and roving bands of outlaws who robbed passengers, stole cargo, dynamited track structures, and disrupted communications. In order to provide adequate protection of goods and passengers from the constant dangers, various States passed railway police acts that enabled private railroads to establish proprietary security forces, with full police powers, for the protection of assets. In many towns and territories, the railway police provided the only protective services until governmental units and law enforcement agencies were established.⁶ By 1914, U.S. railway police numbered between 12,000 and 14,000.⁷ Although railway police have been associated with public law enforcement for a long time, they are, in fact, private security forces granted law enforcement powers.

At the turn of the century, labor unions began to proliferate and to use strikes as a forceful tool for change. Because many factories were located in areas that had no effective public police forces capable of maintaining order, private security agencies were called in by management to quell the disturbances surrounding strikes and to protect lives and property. During this period, two firms were established that are now major security corporations. In 1909, Baker Industries, Inc., entered the first control and burglary detection equipment business. That same year, the head of the FBI's predecessor agency, the Bureau of Investigation, formed the William J. Burns International Detective Agency, now a multi-national corporation with 117 U.S. offices and more than 30,000 employees.

INDUSTRY FORMATION

Prior to and during World War I, the concern for security intensified in American industry, due not only to urbanization and industrial growth but also to sabotage and espionage by politically active nationalists. Security services

⁴ Morn, Frank, "Discipline and Disciplinarians: The Problem of Police Control in the Formative Years," a paper presented at the annual meeting of the American Historical Association, Dec. 28-30, 1975, pp. 5-7.

⁵ Kakalik, J. S., and Sorrel Wildhorn, *The Private Police Industry: Its Nature and Extent*, R-2707/DOJ, Washington, D.C.: Government Printing Office, 1972, Vol. II, pp. 46-49.

⁶ Position paper presented to the Private Security Task Force by the Police and Security Section of the Association of American Railroads, Washington, D.C., Dec. 5, 1975, pp. 2-3.

⁷ Post, Richard S., and Arthur A. Kingsburg, *Security Administration: An Introduction*, Springfield, Ill.: Charles C. Thomas, 1970, p. 5.

expanded to meet the demands, but tapered off when demands lessened after the war, reaching a low point during the Depression era.

At the end of World War I, there were other significant developments in private security. A Burglary Protection Council was formed and held its first meeting in 1921, the results of which thrust Underwriters' Laboratories into the business of establishing specifications for, testing of, and certifying burglar alarm systems and devices.

During the 1940's, World War II proved to be a significant catalyst in the growth of the private security industry. Prior to the awarding of national defense contracts, the Federal Government required that munitions contractors implement stringent and comprehensive security measures to protect classified materials and defense secrets from sabotage and espionage. The FBI assisted in establishing these security programs. Additionally, the Government granted the status of auxiliary military police to more than 200,000 plant watchmen. The primary duties included protection of war goods and products, supplies, equipment, and personnel.⁸ Local law enforcement agencies were responsible for their training. As a result of the heightened emphasis on security within the government/military sphere, industry became increasingly aware of the need for plant security, and its value in protection of their assets.

After the war, the use of private security services and products expanded from the area of defense contractors to encompass all segments of the private and public sectors. For example, in 1954 George R. Wackenhet and three other former FBI agents formed the Wackenhet Corporation as a private investigative and contract security firm. In just 20 years this firm has established itself as the third-largest contract guard and investigative agency in the country. Wackenhet also provides central station alarms, screening of passengers in airports, and most recently, security services for the Trans-Alaska Pipeline.⁹

Wackenhet achieved its growth, in large part, through the acquisition of smaller contract security firms, as did the William J. Burns International Detective Agency. Baker Industries used this technique (notably in the acquisition of Wells Fargo) to expand beyond its electronic detection and equipment origins into guard, armored car, patrol, and investigation services. (Today Baker Industries' security guard and armored car service groups account for about 25 percent of its revenues.) Burns used its acquisitions and industry reputation to move into central station alarms and electronic security equipment. Pinkerton's, on the other hand, concentrated on guard and investigative services and achieved most of its growth internally.¹⁰ Other companies developed along similar lines; these were selected merely to illustrate the historical growth patterns of the earliest private security firms.

Proprietary security, although not as visible as contractual and other forms of security, has experienced equal if not greater growth. From an historical aspect, the greatest growth occurred as a result of World Wars I and II, with the increased governmental concern for heightened security for contractors.

Although no accurate data are available, Federal Government regulation has been a significant factor in the growth of proprietary security over the years. Another major factor has been the increased awareness of companies of the importance of crime reduction and prevention as it relates to company property. In response to this need, both small and large companies have increased proprietary security functions. Thus, it can be concluded that the growth of proprietary security has paralleled that of contractual security.

INDUSTRY COMPOSITION

Several market studies suggest (on the basis of reported earnings of the publicly held corporations engaged in private security) that a half-dozen firms control more than 50 percent of the total market for protective services and products. This statistic, however, does not present the true growth trends that are occurring.

One study indicates that since 1939, when industry records were first kept, more than 2,400 new firms have entered the private security field. The number of such firms doubled in the 9-year period from 1963 to 1972.¹¹ In Figure 6, some of the

⁸ Green and Farber, *op. cit.*, p. 27.

⁹ 1974 Annual Report to Shareholders, the Wackenhet Corporation, Coral Gables, Fla., March 8, 1975.

¹⁰ Kakalis and Wildhorn, *op. cit.*, pp. 40-40.

¹¹ Nossov, W., "The Security Enforcement Industry." Merrick, N.Y.: Morton Research Corporation, October 1975, p. 51.

major firms are categorized according to security service and product lines¹² and shows that several companies are diversified in the types of services that they provide. More importantly, it illustrates that the growth of private security has become technologically intensive over time. A number of firms appearing in Figure 6 were not originally active in the traditional business areas of private security (i.e., guards, investigative, armored car and courier, and central station alarms). Moreover, some of these firms' major activities are in other industries, such as consumer products, electronics, data processing, and engineering.

An analysis of the data from a 1975 security survey in St. Louis (Appendix 2) offers further support that major firms do not control the private security marketplace. This survey indicated that there are only eight major national security firms or their subsidiary companies providing contractual guard, armored car and courier, investigative, and alarms services in this major market area. Their employees represent about 23 percent of the total number (1,962) of contractual, licensed private security personnel in St. Louis supplied by contractual security companies. The remaining 77 percent (1,511) are provided by '78 local contractual security companies.

Sufficient resources were not available to determine if this same situation exists throughout the United States. However, if St. Louis is representative of other market areas throughout the country, it is questionable whether a few major national firms consistently control more than half the total market for protective services and products. The number of guard, investigative, and other protective service contractual firms, as shown in Table 1, also suggest that smaller firms with fewer than 100 employees have experienced significant growth in this area.

Figure 6. Major Publicly Held Firms by Type of Security Product and Services

Contract Guard & Investigative:	Burns Holmes Electric Protective Honeywell Morse Signal Devices Wackenbut
Allied Security ATO (Advance Industry Security) Baker Industries (Wells Fargo) Burns Guardsmark IBI Security Loomis (Stanley Smith Security) Pinkerton's Serviceco (N.B.) Wackenbut Walter Kidde (Globe Security)	ATO Honeywell Johnson Control Pittway (ADEMCO) Walter Kidde Westinghouse
Armored Car Services:	Closed-Circuit TV:
Baker Industries Loomis Pittston (Brinks)	Ampex Babcock and Wilcox Bell and Howell General Electric Honeywell Motorola Panasonic
Fixed Security Equipment:	RCA Sony
American Standard (Mosler) ATO, Inc. Diebold Walter Kidde	
Central Station Alarms:	
ADT Baker Industries	

Source: Research activities of the Private Security Task Force, 1975-1976.

¹² The firms selected for Figure 1 were extracted from listings by the marketing reports of publicly held private security firms that account for a substantial share of the market for security services and product lines. In contract guards and investigators, for example, only those firms annually earning at least \$7 million from these services were listed. These firms collectively, then, would be considered the major firms.

TABLE 1.—NUMBER OF PROTECTIVE SERVICE ESTABLISHMENTS BY SIZE OF EMPLOYMENT

Firm employment	1967	1973	Unit change 1967-73
1 to 3 employees	838	960	+122
4 to 7 employees	443	662	+219
8 to 19 employees	498	874	+376
20 to 49 employees	366	800	+434
50 to 99 employees	172	421	+249
100 to 249 employees	155	294	+139
250 to 449 employees	63	114	+51
500 plus employees	28	57	+34
Total	2,558	4,182	+1,624

Source: "The Security Enforcement Industry," the Morton Research Corp., October 1975.

TECHNOLOGICAL IMPACT

Technology has played an important role in the growth of the private security industry. For example, with the application of advanced technology to the security industry, even one of the oldest security devices, the lock, was subject to revolutionary changes: combination locks, combination time locks, delayed-action time locks, combination locks with surveillance and electronic controls, and eventually access-control systems that use the technology of television and minicomputers.

The same advances in electronics technology that improved the quality of television and radio have had significant impact upon the security market, broadening it to include additional consumer areas. This new technology has fostered the development of large-scale, totally integrated security systems run by computers that control not only access but also refrigeration, heating, air-conditioning, and fire detection. The progression from vacuum tubes to transistors to today's subminiaturization age of hybrid integrated circuit technology has played a major role in the growth of the industry.

Additionally, technological advances have reduced component cost and size, leading to the introduction of security measures now commonly in use, such as low-light-level, closed-circuit television cameras and electronic article-surveillance devices. A number of recent technological advances in electronics and communications engineering have not yet been applied to the development of security products and systems. Electronic security will likely become more prevalent as applications are developed and become cost effective.

Other factors, in addition to the rising crime rate, account for this technologically intensive growth in private security services. For example, the Insurance Services Office recommends that insurance companies offer a premium credit or reduction when commercial and industrial property is protected by burglary and detection systems certified by Underwriters' Laboratories. The Federal Bank Protection Act of 1968 mandated increased security measures and equipment for Federal banks after they had sustained 23 deaths, 61 injuries, and \$15 million in losses from robberies, burglaries, and larcenies in 1967.¹³

In some instances, the sheer magnitude of an organization's assets requires highly sophisticated security measures. For example, various art museums in the United States and Canada employ advanced security technology to protect their \$7 billion collective investment. In fact, nearly half the budgets for special exhibitions at major art museums, as well as 10 to 20 percent of normal operating budgets, are expended for security measures.¹⁴

Most market estimates project that, with the "encroachment by electronic technology,"¹⁵ growth rate for guard, armored car, and courier services will be modest compared to the 10 to 12 percent annual growth of the past few years.

¹³ Davis, Alberts. "Bank Security—It is the Law," *Industrial Security*, October 1969, p. 5.

¹⁴ Pfeffer, Irving, and Ernest B. Uhr, "The Truth About Art Museum Insurance," *Museum News*, Vol. 52, No. 6, March 1974, p. 23.

¹⁵ Little, Arthur D., Inc. "Outlook for the U.S. Safety, Fire Protection and Security Business." Cambridge, Mass.: ADLI, January 1973, p. 23.

INDUSTRY TRENDS AND REVENUES

The private security community is often referred to as the private security industry—and for good reasons. According to one 1974 estimate, expenditures for the provision of private security in this country has reached \$6 billion annually.¹⁶ This figure includes proprietary or inhouse security, as well as contractual private security products and services.

Quantifiable data concerning the size of the private security industry in terms of number of firms, personnel, and revenues vary within the research reports available. This is understandable because very little baseline data are available.

The following estimates give some idea of the magnitude of the security industry: Two recent market research studies place the estimate of security services and products provided to clients by private firms in 1975 at \$3 billion. A study by Arthur D. Little, Inc., also estimated revenues of \$3 billion in 1975 for "security products and services," based upon a growth rate of 12 percent per year.¹⁷ Based upon estimated revenues of \$2.5 billion in 1974 for "loss prevention products and services" and a projected growth rate of 10 percent annually, a study by Frost and Sullivan, Inc., estimated 1975 revenues of \$2.8 billion.¹⁸

In a 1970 study of the nature and extent of private security, the RAND Corporation found that \$3.3 billion was expended in 1969 for "security services within the private sector," including \$1.6 billion for inhouse services.¹⁹ This figure breaks down to \$800 million for equipment, \$540 million for contract guards, \$128 million for armored car service, \$120 million for central station alarms, and \$80 million for investigative services.

Both the Arthur D. Little and Frost and Sullivan market research reports estimated that contract guard, investigative, and armored car and courier services account for approximately one-half of all revenues. A market study by Morton Research Corporation estimated total revenues for the provision of protective services at \$2 billion in 1975, on the basis of total revenues of company growth trends and service sector growth patterns.²⁰

A large number of persons are employed in private security. For example, the *RAND Report* (Vol. I) stated that in 1969, 222,400 persons were employed in proprietary or inhouse security functions and 67,500 as contract guards and investigators.²¹ Frost and Sullivan, in their 1974 study, indicated totals of 226,300 inhouse private security personnel and 71,200 contract guards and investigators.²² The Morton Research Corporation report estimated the total number of private guards, watchmen, private police, and detectives at 350,243 in 1970, using occupational characteristics information from the U.S. Bureau of the Census.²³ This figure apparently includes persons employed in the primary occupation of the categories considered quasi-public police and guards and watchmen employed directly by governmental entities.

Various studies indicate that the number of private security personnel in this country currently by far exceeds the number of local sworn police personnel. For example, a recent study in Cuyahoga County (Cleveland, Ohio) found 8,900 private guards and detectives compared with 4,150 sworn police officers.²⁴ Con-

¹⁶ "The Losing Battle Against Crime in America," *U.S. News and World Report*, Vol. LXXXII, No. 25, Dec. 16, 1974, p. 32.

¹⁷ Little, Arthur D., Inc. op. cit., p. 23.

¹⁸ Frost and Sullivan, Inc., "The Industrial and Commercial Security Market," New York, March 1975, p. 2.

¹⁹ Kakallik, J. S., and Sorrel Wildhorn, "Private Police in the United States: Findings and Recommendations," R-869/DOJ, Washington, D.C.: Government Printing Office, 1972, Vol. I, p. 12.

²⁰ Nossov, op. cit., p. 2.

²¹ Kakallik and Wildhorn, op. cit., p. 11.

²² Frost and Sullivan, Inc., op. cit., p. 116.

²³ Nossov, op. cit., p. 24.

²⁴ Brennan, Dennis T. "The Other Police," Cleveland, Ohio: Governmental Research Institute, 1975.

sidering that 1,000 of those police officers moonlight as private security officers, the number of private security personnel is even larger.

The contention that private security personnel outnumber public law enforcement officers is further supported by the results of Private Security Task Force surveys conducted in two cities—New Orleans and St. Louis.²⁵ Because police department licensing of private security personnel is required in these two cities, it was possible to obtain reasonably accurate figures for the number of licensed private security personnel. This 1975 study revealed that private security personnel outnumber public police. In New Orleans, there were 4,187 licensed private security personnel and 1,418 police officers. In St. Louis, the number of licensed private security personnel was 2,977; commissioned police officers numbered 2,177. In addition to the number of licensed private security personnel, approximately 45 percent of St. Louis police officers (1,000) have approved secondary employment in private security.

During the 15-year period from 1960 to 1975, there was a dramatic 2,312 percent increase in the use of contract guards in St. Louis, as measured by the change in numbers. At the same time, there was a significant decrease in the number of inhouse guards as a percentage of total private security personnel. During this same 15-year period in St. Louis, the number of private security personnel increased 263 percent, while the number of commissioned police officers increased only 11 percent.

The Private Security Task Force also gathered employment figures for private security. (A summary of that effort is in Appendix 9.) The most significant conclusion reached by this research was that there are at least a million persons presently employed in private security.

Although there are problems inherent in comparing sets of figures and determining the validity of data, the important point is that the delivery systems for providing private security services and products are a large-growth industry. Americans are spending increasing amounts of money, over and above public law enforcement expenditures, to protect themselves and their property.

Much of the growth of private security can be attributed to a rising crime rate, coupled with the fact that public law enforcement does not accommodate the specialized needs of business and industry for asset protection. The average annual growth rates of security services and products over the past several years of 10 to 12 percent has approximated the annual increase in the rate of crime, as measured by the FBI Uniform Crime Reports. According to preliminary reports for Crime Index offenses in 1975, crime in the United States rose by 9 percent in 1975, as compared with 1974.²⁶ Robbery and aggravated assault increased 5 percent each; larceny-theft, 12 percent; and burglary, 7 percent.

As crime-related losses in business communities grew to an estimated \$21.3 billion in 1974, total expenditures for security were projected at \$6 billion (contractual and proprietary).²⁷ The sales of contractual security services and products advanced rapidly in the 15-year period from 1958 to 1973: from \$428 million to nearly \$2 billion.²⁸ (See Figure 7.) In the 5 years from 1967 to 1972, total protective service receipts increased from \$522 million to \$1.4 billion.²⁹

As mentioned earlier, market research studies by Arthur D. Little and Frost and Sullivan estimated the 1975 sales for security products and services at approximately \$3 billion. Figure 3 outlines the major user segments of this market. These composite figures are based on the rather consistent market

²⁵ "Characteristics of Licensed Private Security Personnel in Two American Cities: New Orleans, Louisiana, and St. Louis, Missouri." See Appendix 2 to this report.

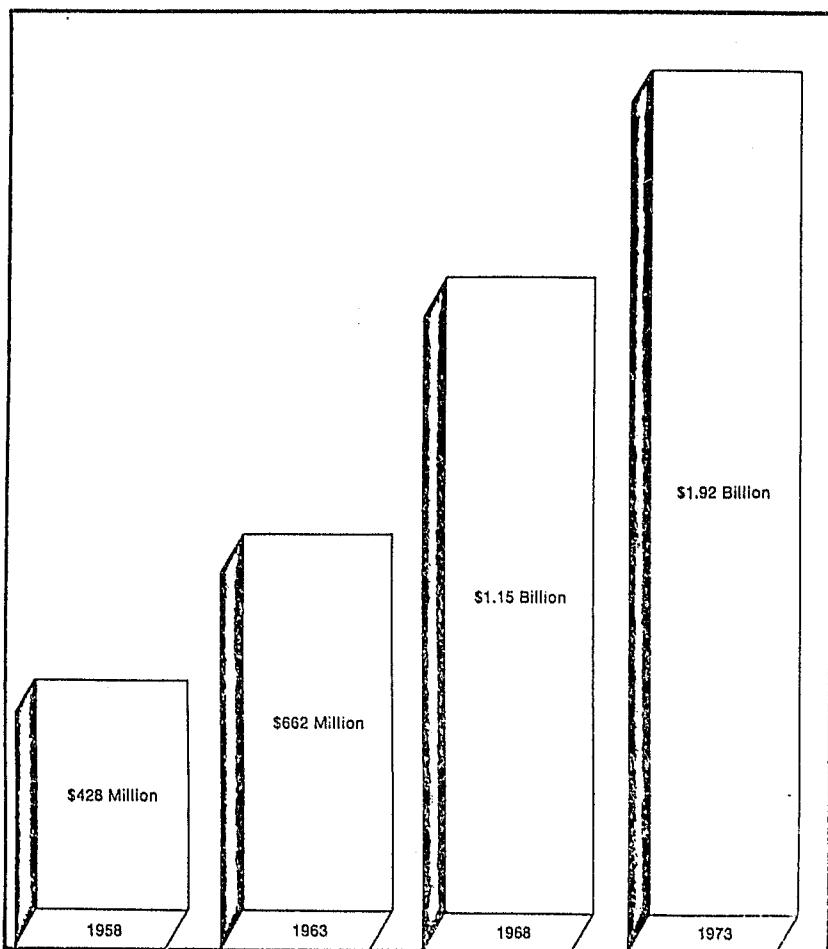
²⁶ "FBI Uniform Crime Reports," January-June 1975.

²⁷ U.S. News and World Report, op. cit., p. 32.

²⁸ Data for Figure 2 was compiled using Predicasts, Inc., data for security services and products, excluding fire-detection equipment. See J. S. Kakalkik and Sorrel Wildhorn, "The Private Police Industry: Its Nature and Extent," R-870/DOJ, Washington, D.C.: Government Printing Office, 1972, Vol. II, p. 31.

²⁹ Nossov, op. cit., pp. 2-3.

Figure 7. Growth of Private Security (Sales of Products and Services)



Source: RAND Corporation, *The Private Police Industry: Its Nature and Extent*, R-870/DOJ. Washington, D.C.: Government Printing Office, Vol. II, 1972, p. 31.

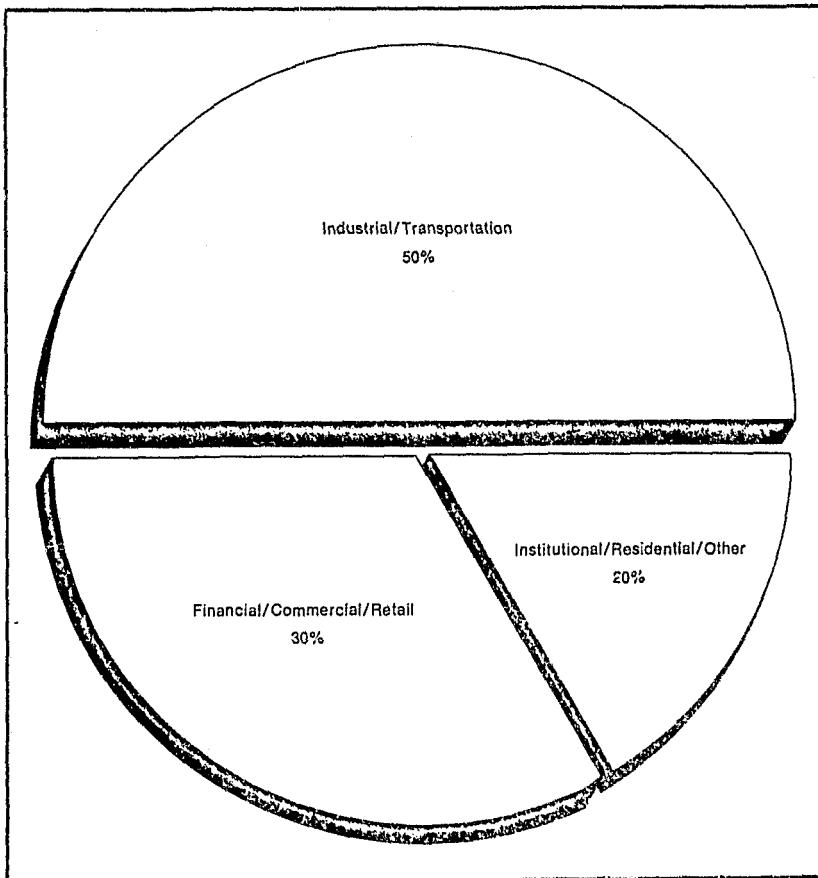
estimates made by Predicasts, Inc., the RAND Corporation, A. D. Little, and Frost and Sullivan.

In reviewing Figure 8, it is significant to note the enormous cost of crime in selected areas of each market segment:

- Industrial and transportation segments account for 50 percent of the total market. The U.S. Senate Select Committee on Small Business fixes annual cargo theft at \$2.5 billion.⁵⁰

⁵⁰ Frost and Sullivan, Inc., *op. cit.*, p. 55.

FIGURE 8.—Major Market Segments for Private Security Products and Services.



• Financial, commercial, and retail interests represent approximately 30 percent of the total market. The U.S. Department of Commerce cites \$6.5 billion in retail losses from crime during 1975,²¹ and the FBI Uniform Crime Reports placed nonresidential losses from burglary at \$423 million in 1974.²² Discount department stores report that losses of cash and merchandise would reach \$845 million in 1975.²³ And the hotel-motel industry estimates millions of dollars lost during 1975 to souvenir hunters alone.²⁴

• Institutional, residential, and other areas comprise the remaining 20 percent of the market. The U.S. Senate Juvenile Delinquency Subcommittee Report estimates that the cost of vandalism in the schools—\$500 million annually—is comparable to the "entire investment for textbooks for our nation's schools."²⁵

The foregoing classification represents those industry segments that have remained the principal users of private security, but the industry has expanded and contracted over time to meet various other demands. For example, railway

²¹ "Crime in Retailing," Washington, D.C.: Department of Commerce, August 1975, p. VII.

²² "FBI Uniform Crime Reports," 1974.

²³ "Store Thieves and Their Impact," Mass Retailing Institute of New York, 1974.

²⁴ "Hotel-Motel Men Suffer in Silence," *Security Systems Digest*, Feb. 13, 1974, p. 1.

²⁵ "School Crime at Crisis Stage," *Chicago Tribune*, January-February 1974, p. 25.

police reached a record number of between 12,000 and 14,000 personnel in 1914 as railroads spread across the country, but their number has now reduced to approximately 3,500.⁵⁶ The use of commercial aircraft skyjacking as a terrorist and extortion technique created an additional need in the transportation industry for private security personnel. The air transport industry has engaged in point-of-departure screening of airline passenger and baggage for explosive devices and weapons at all principal U.S. airports since December 1972. Largely as a result of these mandatory screening procedures, there has not been a successful skyjacking of a commercial aircraft in the United States since their institution.

Terroristic acts, however, have continued to increase in other segments of society. The FBI reported 42 persons killed, 242 persons injured, and \$23.4 million in property damage from 1,574 bombing incidents in the first 9 months of 1975.⁵⁷ These figures show the largest increase in deaths, personal injuries, and property damage since 1972, when the FBI established the National Bomb Data Center to monitor such incidents. A majority of these bombings, especially those involving extensive property damage, were directed against corporations. Companies have had to initiate elaborate, and often costly, procedures to protect their assets and key executives. For example, private security firms, as mentioned in Section 1, provide an estimated 20,000 persons as bodyguards and frequently install electronic devices to aid in protecting corporate executives, other VIP's, and their families and personal property.

Despite its growth, periodic expansion into other areas, and increasingly sophisticated products, the private security industry continues to center most of its services in the areas from which it originated in the 1850s: guards, investigators, and armored car and courier services. These services, according to the Arthur D. Little, Inc., market report, continue to account for nearly 50 percent of industry revenues (Figure 9). The market study by Morton Research estimated the service mix among protective services, based upon the percentage of total receipts by type of service in 1974: detective agencies (including contract guards and watchmen), 61 percent; armored car services, 17 percent; burglar and fire alarm services, 22 percent.⁵⁸

SECURITY TRADE ASSOCIATIONS

The growth of private security services and products has been accompanied by a growth in security-related national trade associations. Currently, there are more than 30 private security trade organizations, plus a number of security committees or divisions of major national associations, such as the American Bankers Association, the Association of American Railroads, the National Association of Manufacturers, the American Hotel and Motel Association, the American Transportation Association, and the National Retail Merchants Association.⁵⁹ (See Appendix 5 for a listing of security-related associations.) There are also numerous State and regional security associations. Functionally, the trade associations cover the full range of private security activities, with one or more in areas such as alarms, armored cars, credit card fraud, private detectives, computer security, educational security, detection of deception, insurance, and security equipment.

The American Society for Industrial Security (ASIS), a professional society with a membership, in June 1976, of about 7,000 security executives, supervisors, and administrators, has made significant contributions to the professionalism of the private security industry. To further the objectives of crime prevention and the protection of assets, ASIS is concerned with all aspects of security in the private sector and emphasizes the education and professionalism of its members through publications, workshops, and seminars. The ASIS Foundation, Inc., was established as a separate organization in 1966 to receive grants and donations for programs to further upgrade security professionalism.

CONCLUSION

Private forces have been used to provide security in America from the earliest colonial times. Even with the establishment of public police forces, many businesses and industries sought the assistance of private security services to provide additional protection for their property and assets. Industrialization, urbaniza-

⁵⁶ American Association of Railroads, *op. cit.*

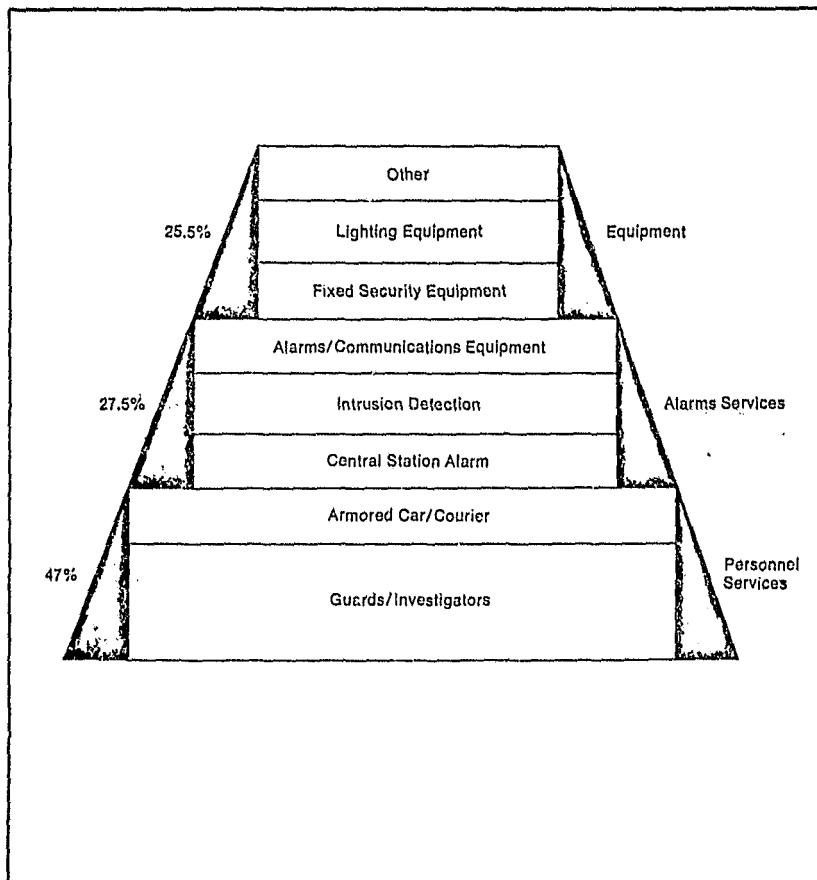
⁵⁷ "FBI National Bomb Data Center Reports," January-September 1975.

⁵⁸ Nossor, *op. cit.*, p. 5.

⁵⁹ "Security Letter," Vol. V, No. 18, Part II.

tion, and prewar and postwar security demands intensified the need for additional protection. Many contractual private security companies and proprietary forces emerged in response to this need, resulting in a substantial growth of the industry. Advances in electronic technology have also contributed significantly to the industry's growth pattern.

FIGURE 9.—Private security products and services revenues.



Source: A. D. Little, Inc., "Estimates of Sales to End User—1975," *Outlook for the U.S. Safety, Fire Protection and Security Business*, January 1973.

Today, as a result of ever-rising crime rates, coupled with the enormous demands placed upon public law enforcement agencies and their lack of adequate resources to deal with these demands, private security has become a multibillion-dollar-a-year industry, and the number of private security personnel surpasses that of public law enforcement in many localities. Moreover, present crime and financial statistics indicate that the industry will continue to experience significant growth in future years. Security trade associations have similarly grown in size and number, and the American Society for Industrial Security has made significant strides toward professionalism of the field.

However, even though it can be established that the investment in private security services and products has grown significantly, very little attention has been devoted to research in this area, accounting for the inability to provide concrete figures on its exact extent and revenues. This paucity of information is highlighted throughout this report in the interest of establishing a reliable data base for future focus on upgrading the industry and its components.



I N D E X

[NOTE.—The Senate Criminal Laws and Procedures Subcommittee attaches no significance to the mere fact of the appearance of the name of an individual or organization in this index.]

A

	Page
American Association for the Advancement of Science.....	111
American Bankers Association.....	140
American District Telegraph Co. (ADT).....	132
American Historical Association.....	132
American Hotel and Motel Association.....	140
American Institute of Marine Underwriters.....	99
American Society for Industrial Security.....	95, 97, 98, 107, 108, 115, 126, 130, 140
Committee on Privacy.....	95
Computer Security Committee.....	95, 108
Transportation and Security Committee.....	98, 99
American Transportation Association.....	140
Cargo Loss Committee.....	99
Association of American Railroads.....	132, 140
"Auditing Around the Computer Center" (article).....	114
Avon Products, Inc.....	95, 107

B

Baird, Lindsay L., Jr.....	95, 96
Testimony of.....	108, 118, 119, 123-125, 127, 128
Baker Industries, Inc.....	132, 133
Bank Security—It is the Law (article).....	135
Banking Act.....	119
Bell, Griffin, Attorney General.....	112
Brennan, Dennis T.....	130
Brink, Washington Perry.....	132
Bureau of the Census.....	136
Bureau of Investigation.....	132
Burglary Protection Council.....	133
Bullock, Mr.....	100

C

Canada.....	135
CBS.....	120
Chicago Tribune (newspaper).....	139
Civil Service Act of 1883.....	132
Civil War.....	132
Cole, Richard.....	102
"Coming: Another Revolution in Use of Computers" (article).....	111
Committee on Government Operations, Senate.....	111
Communists.....	113
Computer Abuse (report).....	111
Computer Security (publication).....	112
Computerworld (publication).....	113, 114
Crime in Commerce (publication).....	139
Crime Control Digest.....	111
Crime Index.....	137

D	Page
Data Management (publication)-----	114
Davis, Alberts-----	135
"Defenseless Society, The" (book)-----	107
Department of Commerce-----	108, 109, 139
Department of Defense-----	116
Department of Health, Education and Welfare (HEW)-----	112, 114
Department of Justice-----	123
Department of State-----	108
Department of Transportation-----	90, 123
Discipline and disciplinarians: The Problem of Police Control in the Formative Years (paper)-----	132
"DP Center Bombings Plague Italy" (article)-----	114
Duckworth, Donald R-----	95, 96
Testimony of-----	97, 101, 117-120, 122, 123, 126, 129
 E	
Eastern bloc-----	106
Englisch, Henry-----	95, 96
Testimony of-----	98, 121, 123-127, 129
Equity Funding Life Insurance-----	110
Europe -----	113
 F	
Fair Credit Reporting Act-----	109
Farber, R. C-----	131, 133
Federal Bank Protection Act of 1968-----	135
Federal Bureau of Investigation (FBI)-----	106, 108, 118, 132, 133, 140
Uniform crime reports-----	137, 139
National Bomb Data Center reports-----	140
Federal Computer System Protection Act of 1977 (S. 1766)-----	118, 119
Federal Government-----	107, 108
Florida, State of-----	100, 101, 118
Fortune 500-----	104
Freedom of Information Act-----	104, 107, 108
Frost and Sullivan, Inc-----	126, 136-138
 G	
Germany -----	126
Governmental Research Institute-----	186
Green, G-----	131, 133
 H	
Hatch, Senator Orrin G-----	95-130
Holmes, Edwin-----	132
Holmes Protection, Inc-----	132
Hotel-Motel Men Suffer in Silence (article)-----	139
"How the Mafia Invades Business" (article)-----	109
 I	
"Identifying Computer Vulnerability" (article)-----	114
Illinois Bureau of Investigation-----	109
Illinois, State of-----	129
Industrial and Commercial Security Market, The (report)-----	136
Industrial Security (publication)-----	135
Insurance Company of North America-----	95, 98
Marine and Aviation Services-----	95, 98
Insurance Services Office-----	185
Interagency Committee on Transportation Security-----	99
Internal Revenue Service (IRS)-----	120
International Association of Chiefs of Police (IACP)-----	109
International Business Machine Co. (IBM)-----	114
Introduction to Security (publication)-----	181

	Page
Japan	126
Juvenile Delinquency Subcommittee, Senate	130

Kakalik, J. S.	132, 133, 136, 137
Kelley, Clarence M.	106
King, Glen D.	109
Kingsburg, Arthur A.	132
Knight and Richardson (authors)	103

Lambie, William K.	107
Larsen, Jan F.	96
Testimony of	115, 119, 127
Law Enforcement Assistance Administration (LEAA)	108, 116
Little, Arthur D., Inc.	135-138, 140, 141
Long Island	126
<i>Lost Battle Against Crime in America, The</i> (article)	136

Martin, David	95
Mass Retailing Institute of New York	130
Massachusetts, State of	104
Morn, Frank	132
Morton Research Corp.	133, 136, 140
Museum News (publication)	135

National Association of Manufacturers	140
National Cargo Security Council	99
National Retail Merchants Association	140
NBC (National Broadcasting Co.)	118
New York, N.Y.	95, 96, 115, 126
North West Police Agency	132
Norton Co.	95, 101, 102, 104-106
Nossov, W.	133, 136, 137, 140
Nyeum, Susan	111

Other Police, The (article)	136
Oura, S. Steven	111
Outlook for the U.S. Safety, Fire Protection and Security Business (publication)	135

Pagano, L. E.	131
Parker, Don B.	110, 111
Peel, J. D.	131
Pfeffer, Irving	135
Pfizer Co.	96, 115, 116
Philadelphia, Pa.	95
Pinkerton, Allan	132
Pinkerton Protection Patrol	132, 133
Port of New York	127
"Ports of the World" (publication)	99
Post, Richard S.	132
Postal Inspection Service	107
President's Privacy Protection Study Commission	109, 123
Privacy Act	104, 107, 109
Private Police Industry, The: Its Nature and Extent (publication)	132, 137, 138
Private Police in the United States: Findings and Recommendations (publication)	136
Private Security (publication)	131
Private Security Task Force (paper)	132, 137
<i>"Protection Management and Crime Control"</i> (article)	102

R	Page
Rand Corp.	136, 137
Rand Report	136
Report of the Task Force on Private Security, National Advisory Committee on Criminal Justice Standards and Goals, Law Enforcement Assistance Administration	131
Ruane, Thomas F. Testimony of	95, 96 107, 120, 126, 127, 129
 S	
School Crime at Crisis Stage (article)	139
Schultz, Richard L.	95-130
Security Administration: An Introduction (publication)	132
Security Enforcement Industry, The (publication)	133
Security Letter (publication)	140
Security Management (publication)	114
Security Management Systems (publication)	131
Security Systems Digest (publication)	139
Security World Publishing Co.	131
Select Committee on Small Business, Senate	138
Short, Robert J.	95
Social Security Administration (SSA)	113, 114
South Africa	104
Stanford Research Institute	110, 111
Store Thieves and Their Impact (article)	139
Story of Private Security, The (publication)	131
Strategic Investigations Unit	118
 T	
"Ten Days to Rip Off Society" (article)	128
"Thievery on the Waterfront" (TV program)	129
Thomas, Charles C.	131, 132
Trans-Alaska Pipeline	133
"Trans-Alaska Pipeline, The" (S. Rept. 95-20)	109
Truth About Art Museum Insurance, The (article)	135
Tyska, Louis	129
 U	
Uhr, Ernest B.	135
Underwriters' Laboratory	133, 135
Union Army	132
United States	97, 101, 116, 123, 126, 129, 135
Customs Office	129
Government	116
Ursie, II, S.	131
U.S. News and World Report	100, 111, 128, 136, 137
 W	
Wackenhet Corp.	133
Wackenhet, George R.	133
Weather Underground	120, 122
Wells Fargo	133
Wildhorn, Sorrel	132, 133, 136, 137
William J. Burns International Detective Agency	132, 133
Worcester, Mass.	95
World War I	132, 133
World War II	133
 X	
"You May Have to Hire Alcoholics or Drug Addicts in the Data Center Unless . . ." (article)	112



E N D