ENSURING THE SAFETY OF OUR FEDERAL WORKFORCE: GSA'S USE OF TECHNOLOGY TO SECURE FEDERAL BUILDINGS

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

APRIL 25, 2002

Serial No. 107–180

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

85–838 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont
(Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

THOMAS M. DAVIS, Virginia, *Chairman*

JO ANN DAVIS, Virginia
STEPHEN HORN, California
DOUG OSE, California
EDWARD L. SCHROCK, Virginia

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

MELISSA WOJCIAK, *Staff Director*
VICTORIA PROCTOR, *Professional Staff Member*
TEDDY KIDD, *Clerk*
MARK STEPHENSON, *Minority Professional Staff Member*

CONTENTS

ENSURING THE SAFETY OF OUR FEDERAL WORKFORCE: GSA'S USE OF TECHNOLOGY TO SECURE FEDERAL BUILDINGS

THURSDAY, APRIL 25, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2 p.m., in room 2154, Rayburn House Office Building, Hon. Thomas M. Davis (chairman of the subcommittee) presiding.

Present: Representatives Thomas Davis, Jo Ann Davis and Turner.

Staff present: George Rogers, Chip Nottingham, and Uyen Dinh, counsels; Victoria Proctor, professional staff member; John Brosnan, consultant; Teddy Kidd, clerk; Mark Stephenson, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. TOM DAVIS OF VIRGINIA. We are going to be voting in about 5 or 10 minutes, so I want to try and get the opening statements out of the way so when we come back we can hear from you. I apologize for that. I think once we start the hearing it will go pretty quickly, but at least let's get the politicians out of it so we can get to the experts.

Good afternoon. I would like to welcome everybody to today's oversight hearing on the General Services Administration's efforts to secure Federal buildings that it owns and leases. We will discuss the advantages and disadvantages of using commercially available security technologies in Federal facilities and the potential concerns that may arise from their implementation.

GSA acts as the Federal Government's property manager and is responsible for ensuring the safety and security of the Federal buildings it owns and leases. After the Oklahoma City bombings in 1995, GSA began a multi-million-dollar program to upgrade the security of its buildings using the criteria in the Justice Department's report titled "Vulnerability Assessment of Federal Facilities." This was the first time that governmentwide security standards were established for public buildings.

The terrorist attacks of September 11th have led to a renewed assessment of the vulnerability of Federal buildings and focus on a new array of security threats. The acquisition of technological upgrades and new technologies are part of the broader effort to com-

bat these threats. And the effective use of these technologies will be critical to our success.

Today, we are going to examine what role technology plays in the security initiatives that GSA is currently implementing in order to protect Federal buildings and the employees who work in them. We will also try to ascertain what barriers may exist in obtaining and implementing the most appropriate and effective technologies.

Since September 11th, life is returning to normal for most Americans. However, for Federal employees, the effects of the attacks are ever present since Federal buildings remain at a heightened state of alert. In fact, each time there has been a terrorist attack on the United States over the last several years, we have seen a visible security increase in and around Federal buildings. Barricades, metal detectors, car searches, ID checks and security cameras have become familiar sights for the average Federal employee.

These new and upgraded security products and services are used to protect employees and visitors, restrict access or detect intruders in Federal facilities. However, their implementation raises a number of concerns. We need to ensure that Federal agencies can achieve a secure work environment while still maintaining an atmosphere of openness.

Furthermore, can advances in technology offer increased security with limited intrusiveness and inconvenience to employees and visitors? For instance, at the Capitol complex, there are elaborate procedures in place to examine packages sent to congressional offices. We reject courier deliveries for safety reasons. Overnight deliveries become over-a-week deliveries. Obviously, this poses an inconvenience to both recipient and sender. Not just an inconvenience, it is a very inefficient way of doing things. It even affected one of our witnesses testifying today. GSA must grapple with these same concerns.

Additionally, Federal agencies have spent significant sums of money improving security measures, particularly in the wake of September 11th. Since the price for a single type of technology can vary widely, agencies must balance costs against the quality of proven security products and services.

There is no question that the Federal Government is capable of providing security. We know we can use brute force to keep people and packages out of buildings. We did it immediately after September 11th. But our real objective should be the utilization of visible and discreet technologies to provide adequate security, thus allowing the government to work effectively and efficiently with minimal disruption, inconvenience and invasiveness.

I understand the sensitive nature of this issue for security professionals. Therefore, I appreciate your willingness and the willingness of our witnesses to testify before our subcommittee today.

[The prepared statement of Hon. Thomas M. Davis follows:]

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

OVERSIGHT HEARING

"Ensuring the Safety of our Federal Workforce: GSA's Use of Technology to Secure Federal Buildings"

OPENING STATEMENT

Thursday, April 25, 2002

2:00 p.m.

Room 2154 Rayburn House Office Building

Good afternoon, I would like to welcome everyone to today's oversight hearing on the General Services Administration's (GSA) efforts to secure federal buildings that it owns and leases. We will discuss the advantages and disadvantages of using commercially available security technologies in federal facilities and the potential concerns that may arise from their implementation.

GSA acts as the federal government's property manager and is responsible for ensuring the safety and security of the federal buildings its owns and leases. After the Oklahoma City bombing in 1995, GSA began a multi million-dollar program to upgrade the security of its buildings using the criteria in the Justice Department's report titled "Vulnerability Assessment of Federal Facilities." This was the first time that government-wide security standards were established for public buildings.

The terrorist attacks of September 11 have led to a renewed assessment of the vulnerability of federal buildings and focus on a new array of security threats. The acquisition of technological upgrades and new technologies are part of the broader efforts to combat these threats. And the effective use of these technologies will be critical to our success.

Today, we are going to examine what role technology plays in the security initiatives that GSA is currently implementing in order to protect federal buildings and the employees who work in them. We will also try to ascertain what barriers may exist to obtaining and implementing the most appropriate and effective technologies.

Since 9/11, life is returning to normal for most Americans. However, for federal employees the effects of the attacks are ever present since federal buildings remain at a heightened state of alert. In fact, each time there has been a terrorist attack on the United States over the last several years, we have seen a visible security increase in and around federal buildings. Barricades, metal detectors, car searches, i.d. checks, and security cameras have become familiar sights for the average Federal employee.

These new and upgraded security products and services are used to protect employees and visitors, restrict access, or detect intruders in federal facilities. However, their implementation raises a number of concerns. We need to ensure that federal agencies can achieve a secure work environment while still maintaining an atmosphere of openness. Furthermore, can advances in technology offer increased security with limited intrusiveness and inconvenience to employees and visitors? For instance, at the Capitol complex, there are elaborate procedures in place to examine packages sent to congressional offices. We reject courier deliveries for safety reasons. Overnight deliveries become over-a –week deliveries. Obviously, this poses an inconvenience to both the recipient and sender. It even affected one of our witnesses testifying today. GSA must grapple with these same concerns.

Additionally, federal agencies have spent significant sums of money improving security measures, particularly in the wake of 9/11. Since the price for a single type of technology can vary widely, agencies must balance cost against the quality of proven security products and services.

There is no question that the federal government is capable of providing security. We know we can use brute force to keep people and packages out of buildings. We did it immediately after September 11th. Our real objective should be the utilization of visible and discreet technologies to provide adequate security, thus allowing the government to work effectively and efficiently with minimal disruption, inconvenience, and invasiveness.

I understand the sensitive nature of this issue for security professionals. Therefore, I appreciate your willingness of our witnesses to testify before the Subcommittee.

Mr. TOM DAVIS OF VIRGINIA. The subcommittee is going to hear from Keith Rhodes, the Chief Technologist at the General Accounting Office; F. Joseph Moravec, the Commissioner of Public Buildings Service from the General Services Administration; GSA supporting witness Wendell Shingler, Director of the Federal Protective Service; John N. Jester, Chief of Defense Protective Services, Department of Defense; Frank R. Abram, the general manager of the Security System Group; and Roy N. Bordes, the president and CEO of the Bordes Group and council vice president of the American Society for Industrial Security.

I ask unanimous consent they be permitted to participate in today's hearing. Without objection, it will be so ordered.

Representative Turner has not arrived here yet, and I will interrupt statements when at he comes so he can make a statement. But I would like to call our panel of witnesses.

As you know, it is the policy of our committee that all witnesses be sworn before they can testify. If you would rise with me and raise your right hand.

[Witnesses sworn.]

Mr. TOM DAVIS OF VIRGINIA. Be seated.

To afford sufficient time for questions, the witnesses will please limit themselves to no more than 5 minutes for any statement. All written statements from witnesses will be made part of the permanent record.

I think I would like to start with Mr. Rhodes and then move straight down to Mr. Moravec, Mr. Jester, Mr. Abram, Mr. Bordes. Thank you for being with us.

STATEMENTS OF KEITH A. RHODES, CHIEF TECHNOLOGIST, U.S. GENERAL ACCOUNTING OFFICE; F. JOSEPH MORAVEC, COMMISSIONER, PUBLIC BUILDINGS SERVICE, U.S. GENERAL SERVICES ADMINISTRATION; WENDELL SHINGLER, DIRECTOR, FEDERAL PROTECTIVE SERVICE, U.S. GENERAL SERVICES ADMINISTRATION; JOHN N. JESTER, CHIEF, DEFENSE PROTECTIVE SERVICE, DEPARTMENT OF DEFENSE; FRANK R. ABRAM, GENERAL MANAGER, SECURITY SYSTEMS GROUP, PANASONIC DIGITAL COMMUNICATIONS & SECURITY CO.; AND ROY N. BORDES, PRESIDENT/CEO, THE BORDES GROUPS, INC., AND COUNCIL VICE PRESIDENT, AMERICAN SOCIETY FOR INDUSTRIAL SECURITY

Mr. RHODES. Mr. Chairman and members of the subcommittee, thank you for inviting me to participate in today's hearing on security technology to protect Federal facilities.

As you stated, the terrorist attacks of September 11th on the World Trade Center and the Pentagon have intensified concerns about the physical security of our Federal buildings and the need to protect those who work in and visit these facilities. These concerns have been underscored by reports of long-standing vulnerabilities, including weak controls over building access.

As you requested, today I will discuss commercially available security technologies that can be deployed to protect these facilities, ranging from turnstiles to smart cards to biometric systems. While many of these technologies can provide highly effective technical controls, the overall security of a Federal building will hinge on es-

tablishing robust risk management processes and implementing the three integral concepts of a holistic security process: protection, detection and reaction.

The 1995 domestic terrorist bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, led to the establishment of governmentwide minimum standards for security at all Federal facilities. Among the minimum standards for buildings of a higher risk level are security technologies including closed circuit television surveillance cameras, intrusion detection systems with central monitoring capability and metal detectors and x-ray machines to screen people and their belongings at entrances to Federal buildings.

While minimum standards are necessary, no one should assume a false sense of security. Security is not perfect, as evidenced by testing. The GAO's Office of Special Investigations has done, in ongoing requests from Congress, testing the effectiveness of security at Federal buildings.

The key here is risk management. Risk management is the foundation of effective security. In risk management, there are basically five seemingly simple questions that are rather complex to answer.

First question is, what am I protecting? That is, what is the asset I am protecting and how am I valuing it? What would the impact be of its loss? Who are my adversaries? I have to figure out who my opponent is, do I have an adversary, does that adversary have the ability to attack me, and does the adversary have the intent to attack me. How am I vulnerable?

This is where GAO's Office of Special Investigations work comes in, from our standpoint, in that we go out and test the security of Federal facilities to see how they are vulnerable.

What are my priorities? Priorities are what do I want to protect first, second, third and last; and what can I do is actually a two-step question. The first part of the question of what I can do is, what are the countermeasures I can put in place to protect the environment? The second is, what can I afford to do?

All of these questions have to be set up in a structure of protection, detection and reaction. Protection is the actual physical protection of the facility, talking about turnstiles and guards and Jersey barriers and things like that as well as access control. Detection is, once those systems have been breached, how do I know that they have been breached? What is going to let me know that something has gotten through the system without authorization? And reaction is, how is the organization established and how is security established in order to react to breach of security?

One point I would like to make is that reaction—if reaction does not culminate in the use of a guard or a human being, the reaction has been proven to be ineffective. If people here fire an alarm but the fire department doesn't show up, that is ineffective reaction. Likewise, if someone breaks into a building or tries to break into a building and guards do not respond, that is also ineffective reaction.

In looking at the technology itself, technology breaks down into three basic areas: access control, detection and intrusion detection. Detection in this case is detection of weapons or explosives or contraband of some kind.

In the area of access control, there are biometrics. Biometrics are items that belong—that are on a human being himself or herself—a fingerprint, hand geometry, scan of the retina or a scan of the iris, facial recognition, trying to figure out the facial geometry, speaker recognition, voice pattern recognition or signature recognition. These are considered things—because they are biometric, these are things that someone cannot lose. They always have them with them.

The second step in access control is an access card. First part of that is a magnetic swipe using something that looks like a credit card with a magnetic strip on it. You run it through a mag swipe reader and grants you access. Usually, that is associated with the application of a four-digit personal ID number.

There are also proximity cards which have a little wireless communication in it. You get near the proximity reader and the reader will either grant you access or not.

Then, finally, there are smart cards. Smart cards have embedded integrated circuits, actual computer chips in them that contains a wide range of information associated about the individual—access level. It will also give people particular access to rooms.

Associated with access control, there is usually a key pad entry system which looks like a digital phone face, usually has ten numbers or nine numbers on it and a send key. You put in your four-digit personal identification number or however long the ID number is and hit enter and then a door may open.

However, these biometric devices do need to be associated with an access barrier. It is not any good if I can walk by a proximity reader and just keep walking. There has to be something to stop me from getting in. These are usually turnstiles or can be revolving doors.

Next area is detection. This is what most people end up going through at airports. You come in and you walk through a magnatometer, a metal detector. Metal detector will find out if you have any metal on you. If you have metal on you that reaches a certain threshold set by the turnstile or by the magnatometer, then they will order a secondary check.

X-ray machines, this is probably familiar to everyone at airports. Also when your bag passes through an x-ray machine so they can look either for weapons or they can look for explosives or they can look for sharp objects in your bag.

Finally, there are explosive detectors. Sometimes when I have gone to the airport, for example, and gone on an overnight trip somewhere, they have taken my bag and you will see sometimes they will wipe a swab on the strap of the bag and run into a system that checks for evidence of explosive material.

Then, finally, there is intrusion detection, which focuses mainly on closed circuit television or intrusion sensors that track motion.

All of these technologies are available today. Some are varying quality. Some, as you pointed out, Mr. Davis, can be extremely expensive. But no one of the technologies is going to solve all the access control problems or security problems, and technology alone is not going to be the only thing that we can apply to secure a facility. We have to have human beings in the loop who can respond. All of these must work together.

Some of the limitations of the technology are, of course, technology can't compensate for human failure or ineffective security processes. Training of security personnel is vital. The training of the personnel is vital, and the retention of the personnel is vital.

Very often, the government ends up being the great training ground for other organizations. We train security personnel in the military and we train security personnel through GSA or other government organizations only to lose them to either other departments and agencies in the government or we lose them to the private sector.

Technology can also be overestimated. There has to be a healthy "buyer beware" in terms of the viability of the technology. But this is also two-way. Technology bought without an understanding of a department or agency's requirements for security is not the vendor's fault. If the department or agency hasn't laid out their requirements properly and they have just gone and bought technology when they saw what they considered to be an ill-defined problem, then it is not the vendor's fault that the technology does not work. Likewise, if they do establish good requirements and they haven't tested the equipment properly, that is also a problem.

Sometimes a nontechnical solution may be best. Sometimes dogs can sniff out bombs better than technology.

Lack of standards also impedes system integration. A lot of these devices are built by different companies, and therefore it's difficult to integrate the information together into a single system.

And, as you pointed out, there are concerns by the user population about the personal intrusion on their privacy in the use of this technology. For example, just as a side comment before I close, fingerprint technology, even though it's probably the most robust biometric device is resisted by the majority of the population because it's association with law enforcement fingerprinting. So there are nonobvious resistance indicators to the technology.

To close, I would just point out that there are a myriad of technologies available. However, if these technologies are—if the requirements for security are not clearly understood by the department or agency, then the benefits of the technology are overcome.

Thank you very much, and I await any questions from the committee.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Rhodes follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
2:00 EDT
Thursday,
April 25, 2002

DRAFT

NATIONAL PREPAREDNESS

Technologies to Secure Federal Buildings

Statement of Keith Rhodes
Chief Technologist

GAO-02-481T

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on security technologies to protect federal facilities. The terrorist attacks of September 11 on the World Trade Center and the Pentagon have intensified concerns about the physical security of our federal buildings and the need to protect those who work in and visit these facilities. These concerns have been underscored by reports of long-standing vulnerabilities, including weak controls over building access.

As you requested, today I will discuss commercially available security technologies that can be deployed to protect these facilities, ranging from turnstiles, to smart cards, to biometric systems. While many of these technologies can provide highly effective technical controls, the overall security of a federal building will hinge on establishing robust risk management processes and implementing the three integral concepts of a holistic security process: protection, detection, and reaction.

First I will provide an overview of the technologies that provide protection, detection, and reaction capabilities against the most prevalent threats. I will describe the characteristics and capabilities of each of these technologies and summarize their effectiveness, as well as their maturity and other performance factors to be considered in implementing them. While not endorsing any product, I will also identify vendors and costs, and provide examples of sites where they have been deployed. Finally, I will discuss the considerable technical challenges and user acceptance issues still ahead in their implementation.

In conducting our review, we interviewed officials at federal agencies responsible for the physical security of their buildings, including the General Service Administration's (GSA) Federal Protective Service, the Defense Protective Service, the U.S. Capitol Police, and GAO's own Office of Safety and Security. To understand the availability and effectiveness of newer security technologies, we also met with officials from GSA's General Products Center and technologists from the National Institute of Justice's Office of Science and Technology, the Department of Defense's (DoD) Biometrics Management Office, and the Biometrics Foundation. We coordinated with the Security Industry Association and its advisory councils that represent the different security industries within the scope of our work. They provided us with valuable information and contacts. We attended the Biometric Consortium Conference and the International Security Conference and Exposition, where newer technologies were demonstrated and where we discussed aspects of the technologies with industry representatives. We also discussed the results of several of the Federal Aviation Administration's biometric prototype initiatives with program managers. We relied on previous GAO work on physical building security. To familiarize ourselves with available security products, we also

conducted an extensive literature search and obtained and perused technical studies performed by independent organizations and compared their results with vendor-provided information. We performed our audit work from February through April 2002 in accordance with generally accepted government auditing standards.

BACKGROUND

It is the federal government's responsibility to assure the physical protection of its facilities and the safety of employees and visitors of those federal buildings. GSA, through its Public Building Service (PBS) is the primary property manager for the federal government, owning or leasing 39 percent of the federal government's office space. Approximately one million federal employees, millions of visitors, and thousands of children and their day-care providers enter these facilities each day. Within PBS, the Federal Protective Service is responsible for the security of most GSA-managed buildings.

Over thirty other executive branch agencies, including DoD and the departments of State, Veterans Affairs, and Transportation, have some level of authority to purchase, own, or lease office space or buildings. These agencies are responsible for the security of their own sites. The U.S. Secret Service is in charge of the security of the White House and other executive office buildings. The U.S. Capitol Police secures the security of the Capitol complex, which includes the Capitol and House and Senate office buildings. The marshal of the Supreme Court and the Supreme Court Police tend to the security of the Supreme Court. Marshals from the Department of Justice's U.S. Marshals Service ensure the security of other federal courts.

Security Issues Have Been Reported at Federal Buildings

The 1995 domestic terrorist bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, aroused governmentwide concern about the physical security of federal buildings. One day after the bombing, then President Clinton directed Justice to assess the vulnerability of all federal office buildings in the United States, particularly to acts of terrorism and other forms of violence. Justice led a working group in developing a report that established governmentwide minimum standards for security at all federal facilities.[1] That same year the president directed executive departments and agencies to upgrade the security of their facilities to the extent feasible based on the

[1]The report, entitled *Vulnerability Assessment of Federal Facilities*, June 28, 1995, classified federal facilities into 5 security levels ranging from a level 1,with minimum security needs, to a level 5, with high security needs. Fifty-two increasingly stringent security standards were recommended, depending on the level of risk assigned to the building.

report's recommendations, giving GSA this responsibility for the buildings it controls. The report specified security technologies among these minimum standards for buildings of a higher risk level, including closed-circuit television (CCTV) surveillance cameras, intrusion detection systems with central monitoring capability, and metal detectors and x-ray machines to screen people and their belongings at entrances to federal buildings.

In June 1998, we testified on GSA efforts to improve federal building security.[2] We reported that although GSA had made progress implementing security upgrades in its buildings, GSA did not have the valid data needed to assess the extent to which completed upgrades had helped to increase security or reduce vulnerability to the greatest threats to federal office buildings. We also expressed concerns about whether all GSA buildings had been evaluated for security needs. We recommended that GSA correct the data in its tracking and accounting systems, ensure that all GSA buildings were evaluated, and develop program goals, measures, and evaluations to better manage its security enhancement program. In October 1999 we again testified on GSA's efforts. During this review, we found that the accuracy of GSA's security upgrade tracking system had improved and that almost all of its buildings had been evaluated for security needs.

However, a review we performed in April and May 2000 exposed a significant security vulnerability in the access controls at many government buildings.[3] Posing as law enforcement officers, we gained access to 18 federal facilities, where we reached the offices of 15 cabinet secretaries or agency heads. Our briefcases were not searched for weapons or explosives.

As mentioned previously, last September's terrorist attacks against the World Trade Center and the Pentagon have focused even greater security concerns about federal buildings. However, despite a show of increased security, it remains uncertain whether effective countermeasures have actually been implemented. For example, reporters who visited a number of government agencies in late October demonstrated that, without thorough screening, nonemployees could easily gain access to freely wander the buildings.

Concerns about potential threats have prompted federal officials to create a more stringent security environment at federal facilities. For example, the Federal Emergency Management Administration recently informed GSA officials that it was canceling plans to move its national headquarters and 1,000 workers to the Potomac Center redevelopment near Washington D.C.'s

---

[2]U.S. General Accounting Office, *General Services Administration: Many Building Security Upgrades Made But Problems Have Hindered Program Implementation*, GAO/T-98-141 (June 4, 1998) and *General Services Administration: Status of Efforts to Improve Management of Building Security Upgrade Program*, GAO/T-GGD/OSI-00-19 (Oct. 7, 1999).
[3]U.S. General Accounting Office, *Breaches at Federal Agencies and Airports*, GAO/T-OSI-00-10 (May 25, 2000).

waterfront. Citing security concerns about the new building, the agency backed out of a 10-year lease.

Since the 1995 Oklahoma City bombing, the federal government has already spent more than $1.2 billion on increased security measures for the federal government's office space. Following the September 11th terrorist attacks, increased resources have been appropriated for this purpose. Specifically, on September 18, 2001, President Bush signed the Fiscal Year 2001 Emergency Supplemental Appropriations Act (P.L. 107-38), appropriating $40 billion in monies to respond to the terrorist attacks. The act provides funding to cover the physical protection of government facilities and employee security. On September 21, 2001, the president allocated $8.6 million from this appropriation to GSA's Federal Buildings Fund to provide increased security for federal buildings. On October 17, 2001, the president requested that Congress increase the total to $200.5 million for the Federal Building Fund for additional security services at federal buildings. The president's fiscal year 2003 budget requests that $367 million be made available from the Federal Building Fund to fund costs associated with implementing security improvements to federal buildings.

On March 21, 2002, the Bush administration asked Congress for an additional $27.1 billion in emergency funding for fiscal year 2002 for needs stemming from the September 11th terrorist attacks, $5.5 billion of which were for domestic security. Some of these requested funds will most likely be invested in technologies to enhance building security. It will be important to ensure that the technologies that these funds are spent on are effective.

RISK MANAGEMENT IS THE FOUNDATION OF EFFECTIVE SECURITY

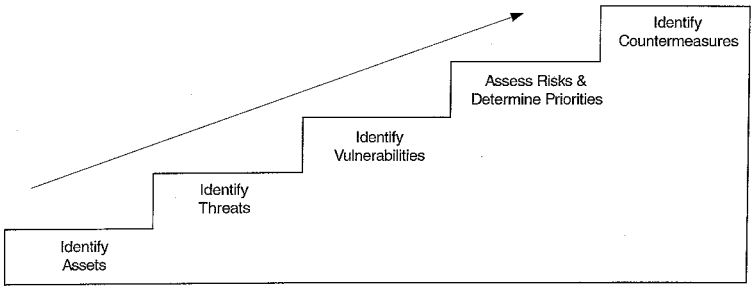
The approach to good security is fundamentally similar regardless of the assets being protected. As GAO has previously reported for homeland security[4] and information systems security,[5] applying risk management principles can provide a sound foundation for effective security whether the assets are information, operations, people, or federal facilities. These principles, which have been followed by members of the intelligence and defense community for many years, can be reduced to five basic steps that help to determine responses to five essential questions.

Because of the vast differences in types of federal facilities and the variety of risks associated with each of them, there is obviously no single approach to security that will work ideally for all buildings. Therefore, following these basic

[4] U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Oct. 31, 2001).
[5] U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68, (May 1998).

risk management steps is fundamental to determining security priorities and implementing appropriate solutions.[6]

Figure 1: Five Steps in the Risk Management Process



What Am I Protecting?

The first step in risk management is to identify assets that must be protected and the impact of their potential loss. Included among the assets of federal facilities are the physical safety and peace of mind of the occupants, the value of the structure itself, and the importance of the mission of the organization housed in the facility. The symbolic value of certain landmark federal facilities and monuments must also be considered in the assessment.

Who Are My Adversaries?

The second step is to identify and characterize the threat to these assets. Is the threat, for example, that unauthorized individuals can gain access to the building to commit some crime, or that an authorized yet disgruntled employee intent on causing harm to fellow employees or the facility can get in, or, still more menacing, that a terrorist will introduce a chemical/biological agent or even a nuclear device into the building?

[6]GSA's building security upgrade program uses a risk assessment approach whereby threats and vulnerabilities are identified and corresponding security countermeasures are identified to either reduce or eliminate each threat and vulnerability.

The intent and capability of an adversary are the principal criteria for establishing the degree of threat to these assets. The terrorist bombing of the World Trade Center in 1993, the Oklahoma City bombing of the Alfred P. Murrah Federal Building in 1995, the U.S. embassy bombings in Tanzania and Kenya in 1998, and last year's September 11th terrorist attacks on the Pentagon and the World Trade Center leave no doubt as to the existence of adversaries intent on causing the maximum harm. And, as these events have tragically demonstrated, our adversaries certainly have the capability. Moreover, more recent information gathered by intelligence and law enforcement agencies have led government officials to believe that both foreign and domestic terrorist groups continue to pose threats to the security of our nation's infrastructure, including our public buildings.

How Am I Vulnerable?

Step three involves identifying and characterizing vulnerabilities that would allow identified threats to be realized. In other words, what weaknesses can allow a security breach? For a facility, weaknesses could include vulnerabilities in the physical layout of the building, its security systems, and processes. For example, the lack of a standoff distance between vehicle access and the building itself, which would allow an adversary to detonate a car or truck bomb within a dangerous distance of the building, is an example of a vulnerability in the perimeter security of a building. Or, it might be that an antiquated and labor-intensive access control system in combination with an inadequate security guard force create weaknesses in security systems and processes that allow entrance to a building.

What Are My Priorities?

In the fourth step, risk must be assessed and priorities determined for protecting assets. Risk entails assessing the potential for the loss of or damage to an asset. Risk levels are established by assessing the impact of the loss or damage, threats to the asset, and vulnerabilities. For example, poor access controls at federal facilities would pose a lower risk of loss of human life on weekends when fewer people are working in the buildings than on weekdays during standard office hours.

What Can I Do?

The final step is to identify countermeasures to reduce or eliminate risks. In doing so, the advantages and benefits of these countermeasures must also be weighed against their disadvantages and costs.

Many security technologies were developed in a research environment. However, in a real-world environment, some degree of security must be traded off against operational and safety considerations. Extreme security

countermeasures cannot be implemented if they could disrupt operations or adversely affect the safety of the occupants of a building. For example, an access control system that uses draconian methods to screen employees at public entrances would be inappropriate except in buildings at the highest risk level because it would cause maximum inconvenience to large numbers of building occupants at peak traffic hours. Moreover, an access control system cannot be so rigid that it impedes the safe exit of a building's occupants during emergencies, such as a fire. In all cases, an acceptable balance between security and these competing factors must be reached, which can only be decided by the building's occupants.

PROTECTION, DETECTION, AND REACTION ARE INTEGRAL SECURITY CONCEPTS

Countermeasures identified through the risk management process support the three integral concepts of a holistic security program: protection, detection, and reaction. Protection provides countermeasures such as policies, procedures, and technical controls to defend against attacks on the assets being protected. Detection monitors for potential breakdowns in protective mechanisms that could result in security breaches. Reaction, which requires human involvement, responds to detected breaches to thwart them before damage can be done. Because absolute protection is impossible to achieve, a security program that does not also incorporate detection and reaction is incomplete.

To be effective, all three concepts must be elements of a cycle that work together continuously. To illustrate, suppose that the **protection** of a side door of a federal building is provided by a lock, which is wired to an intrusion **detection** sensor, which triggers an alarm to alert a guard to initiate a **reaction**. If someone picks the lock, thereby tripping an alarm, and a guard is monitoring the detection system in real time, she or he will detect the incident and can react to contain the intrusion and to apprehend the intruder before damage is done. However, if no guard is monitoring the intrusion detection systems to react to the intrusion, the process breaks down and the security of the building may be compromised. In other words, technologies that implement the concepts of protection and detection cannot alone safeguard a building. An effective human reaction is essential to the security process.

MYRIAD COMMERCIALLY AVAILABLE SECURITY TECHNOLOGIES SUPPORT SECURITY CONCEPTS

Myriad security technologies, at various stages of commercial development, support the security concepts of protection, detection, and reaction. We have categorized these systems according to the particular concept that they support. Access control systems provide protection by establishing a checkpoint at entry points to a building through which only authorized persons

may pass. Detection systems look for dangerous objects and agents on persons, their belongings, and their vehicles at a building's entry points. Intrusion detection systems monitor for security incursions throughout a building to alert security staff to react to investigate and contain the intrusion.

Access Control Systems

The first line of security within a federal building is to channel all access through entry control points where identity verification devices can be used for screening. These devices "authenticate" individuals seeking entry, i.e., they verify that the individuals are indeed authorized to be there by electronically examining credentials or proofs of identity.

Identity verification devices use three basic technological approaches to security based on something you have, something you know, and something you are. Accordingly, they range from automatic readers of special identification cards (something you have), to keypad entry devices that generally require a pin number or password (something you know), to more sophisticated systems that use biometrics (something you are) to verify the identity of persons seeking to enter a facility. More secure access control systems use a combination of several of these approaches at the same time for additional security.

Technologies used by identity verification devices include the basic bar code or magnetic strip for card-swipe readers, similar to those used for credit cards, cards that use radio frequency signals and need only be passed within close proximity to a reader to identify the card holder, and smart cards that contain biometric identifiers. Keypad entry devices are often used in combination with cards and card readers. Newer access control systems that use biometric technologies to verify the identity of individuals seeking access can significantly increase building security.

The term biometrics covers a wide range of technologies used to measure and analyze human characteristics to verify identity. Identifiable physiological characteristics include fingerprints, eye retinas and irises, and hand and facial geometry. Identifiable behavioral characteristics are speech and signature. Biometrics theoretically represent a very effective security approach because biometric characteristics are distinct to each individual and, unlike identification cards and pin numbers or passwords, they cannot be easily lost, stolen, or guessed.

Biometric systems first capture samples of an individual's unique characteristic that are then averaged to create a digital representation of the characteristic, known as a template. This template is stored and used for comparison to determine if the characteristic of the individual captured by the identity verification device at the entry control point matches the stored

template of that individual's characteristic. Templates can be stored within the device itself, in a centralized database, or on a "smart" card.

Until recently, in addition to being very expensive and requiring enormous computing power, the performance of most biometric technologies had unreliable accuracy. However, prices have significantly decreased and, after years of research, the technology has recently improved considerably. Today biometric devices that read fingerprints and hand geometry have been operationally deployed and proven to be affordable and reliable. Nevertheless, other biometric technologies are not as mature and still tend to falsely reject authorized persons or falsely accept unauthorized persons. These reliability weaknesses will have to be overcome before their use can be widespread. User acceptance is also an issue with biometric technologies in that some individuals find them difficult, if not impossible, to use. Still other individuals resist biometrics in general because they perceive them as intrusive and infringing on their right to privacy.

Once a person is authenticated, access control systems are designed to electronically allow passage through some barrier. Building access barriers can range from such evident physical structures as revolving doors to all but transparent optical turnstiles that generate an alarm when an unauthorized individual attempts to pass.

Table 1 provides a high-level description of access control technologies that can be deployed to protect federal facilities. Attachment I describes the technologies in greater detail.

Table 1: Access Control Technologies

Access Control Technologies					
		How the technology works	**Effectiveness**	**Performance factors**	**User acceptance**
Biometric Technologies	**Fingerprint scan**	Patterns of fingertips captured and compared	Reliable	Dirty, dry, worn fingertips	Some resistance based on association with law enforcement
	Hand geometry	Dimensions of hand and fingers measured and compared	Fewer unique characteristics measured	Injuries and jewelry	Good, but may require minimal training
	Retina scan	Patterns of blood vessels on retina captured and compared	One of most accurate biometrics	Hardest to use of biometric technologies	Considered intrusive
	Iris scan	Patterns of iris captured and compared	One of most accurate biometrics	Lighting and movement	Some resistance based on sensitivity of eye
	Facial recognition	Facial features captured and compared	Dependent on lighting, positioning, updating reference template	Environmental factors	Good, but some concern about possible misuse
	Speaker recognition	Cadence, pitch, and tone of vocal tract captured and compared	Better suited for other applications	Environment, inconsistencies, and quality of equipment	Good
	Signature recognition	Rhythm, acceleration, and pressure flow of signature captured and compared	Better suited for other applications	Erratic signatures	Good
Magnetic swipe cards		Identification encoded in magnetic strip on plastic card	Substantially more secure if used in conjunction with other controls	Subject to demagnetization and wear and tear	Good
Proximity cards		Identification encoded in card transmitted by radio frequency antenna	Substantially more secure if used in conjunction with other controls	More durable than swipe cards	Good
Smart cards		Identification data stored in memory chip	Substantially more secure if used in conjunction with other controls	Requires proper care	Some concern about security of data stored on card
Keypad entry systems		Require users to enter passcodes	Substantially more secure if used in conjunction with access card system	Users may forget passcodes; vulnerable to malfunction and vandalism	Good
Access Barriers (Turnstiles/Revolving doors)		Used in conjunction with access card systems to bar unauthorized access	Only allows authorized access	High throughput	Good

Detection Systems

Detection systems provide a second layer of security. Portal (walk-through) metal detectors can be strategically deployed at entry control points to screen individuals for hidden firearms and other potentially injurious objects, such as knives and explosive devices, as they clear the access control system. Unlike more traditional detectors which simply generated an alarm when a metal target was detected anywhere on an individual's body, more technologically advanced portal scanners now come equipped with light bars to highlight the locations where highest metal concentrations are detected. More sensitive and ergonomic handheld detector wands are also now commercially available to perform thorough and rapid follow-up screens.

As individuals proceed through the metal detector, their carried items can be passed through an x-ray system, which scans the items to obtain an image of the contents. Low-energy x-ray systems are also currently being tested to screen individuals for hidden weapons and explosives. However, performance, privacy, and health issues associated with this technology will have to be overcome before it can be widely deployed. Though not yet commercially available, holographic scanning, which can screen for metallic as well as nonmetallic weapons concealed under clothing, is another new technology currently being tested by the Federal Aviation Administration.

Explosive trace detectors provide an additional layer of building security. Security personnel swab the surface of a person's belongings at entry control points to check for concealed explosives. The swab is then placed into the detection device, which tests for the presence of explosive traces. Portal explosive detection systems and large vehicle-bomb detection systems are now commercially available, but the technology has not yet been widely deployed. Finally, more research and development efforts will be required before technologies for detecting chemical/biological agents become more effective and affordable.

Table 2 provides a high-level description of detection technologies that can be deployed to protect federal facilities. Attachment II describes the detection technologies in greater detail.

Table 2: Detection Technologies

Detection Technologies				
	How the technology works	**Effectiveness**	**Performance factors**	**User acceptance**
X-ray machines	Electromagnetic waves (X-rays) are used to allow distinct structures to be viewed on a monitor. Due to differences in material compositions, items are distinguishable.	Persons familiar with the exact construction of a particular X-ray system could pack a bag to make a threat item difficult to recognize.	Performance depends on the efficiency of the operator and the amount of clutter in a bag or on a person.	Some concern about exposure to radiation.
Metal detectors	Used to locate concealed metallic weapons on persons. When the detector senses a questionable item or material, an alarm signal is produced.	Considered a mature technology. Can accurately detect the presence of most types of firearms and knives. However, they are typically not accurate when used on objects that contain a large number of different materials.	Can be extremely sensitive to interference from conflicting signals of nearby objects. Throughput depends on well-trained and motivated operators. Portal detectors require frequent adjustment.	Some concern about exposure to the magnetic field of metal detectors. Issues of privacy and discrimination have also been raised.
Explosive detectors	Used to detect bulk or trace explosives concealed in, on, or under vehicles, containers, packages, and persons.	Technology capable of detecting most military and commercially available explosives. However, most systems designed to detect only a subset.	Depends on the method used to collect sample and operator efficiency.	Explosive detection units are not intrusive.

Intrusion Detection Systems

Intrusion detection systems serve to alert security staff to react to potential security incidents. CCTV cameras play an integral part of intrusion detection systems. Security personnel can use this technology to monitor activity throughout a building, in particular at entryways, exits, stairwells, and other areas that are susceptible to intrusion. CCTV technology is mature, practical, and reasonably priced. Moreover, it is highly cost efficient because one person can monitor several areas on different screens at the same time from one central location. However, experiments have shown that relying on security

staff to detect incidents by constantly monitoring scenes from the camera in real time is ineffective. Because watching camera screens is both boring and mesmerizing, the attention of most individuals has degenerated to well below acceptable levels after only 20 minutes of viewing. This is particularly true if staff are watching multiple monitors simultaneously. A more practical application of CCTV is to interface the CCTV system with electronic intrusion detection technologies, which alert security staff to potential incidents requiring monitoring.

Electronic intrusion detectors are designed to identify penetrations into buildings through vulnerable perimeter barriers such as doors, windows, roofs, and walls. These systems use highly sensitive sensors that can detect an unauthorized entry or attempted entry through the phenomena of motion, vibrations, heat, or sound. Examples are technologies that detect motion through breaks in a transmitted infrared light beam and heat emitted from a warm object, such as a human body.

When an intrusion is sensed, a control panel to which the sensors are connected transmits a signal to a central response area, which is continually monitored by security personnel. The sensor-detected incident will alert security personnel of the incident and where it is occurring so that personnel will know what monitor to pay attention to. By interfacing these technologies, security personnel can initially assess sensor-detected security events before determining how to react appropriately. Alarm-triggered video recorders can also be installed to provide immediate playback of a detected event for analysis.

Table 3 provides a high-level description of intrusion detection technologies that can be deployed to secure federal facilities. Attachment III describes the technologies in greater detail.

Table 3: Intrusion Detection Technologies

Intrusion Detection Technologies				
	How the technology works	**Effectiveness**	**Performance factors**	**User acceptance**
CCTV	A visual surveillance technology for monitoring a variety of environments and activities. Typically involves a dedicated communications link between cameras and monitors.	The clarity of the pictures and feed can be excellent. Cameras vary in size, light sensitivity, resolution, type and power.	Often not effective as an active surveillance tool because of security staff's inattention	Concern about misuse to track people, racially discriminate, and engage in voyerism.
Intrusion sensors (line sensors, video motion detectors, balanced magnetic switches, and sonic and vibration sensors)	Detects penetrations into secure areas through walls, roofs, doors, and windows. Detection is usually reported by an intrusion sensor and announced by an alarm, which must be followed by a human assessment to determine proper response.	Reliable	Susceptible to nuisance alarms which can be generated by animals, blowing debris, lightning, water, and nearby traffic. Any disturbance in the electrical power will affect performance.	Users cannot freely open and close windows and doors that have been equipped with sensors.

TECHNOLOGY IS NOT A PANACEA

Although the newer technologies can contribute significantly to enhancing building security, it is important to realize that deploying them will not automatically eliminate all risks. Effective security also entails having a well-trained staff to follow and enforce policies and procedures. Moreover, the technical capabilities of security systems must not be overestimated. Finally, a broad framework of supporting functions must be in place at the federal, state, and local levels.

Technology Cannot Compensate for Human Failure or Ineffective Security Processes

Good security requires technology and people to work together to implement policies, processes, and procedures that serve as countermeasures to identified risks. To illustrate this point, let us examine the following scenario: an organization has policies in place to mitigate the risk of an outsider committing

a harmful act against its employees. One policy states that entry to the building is restricted to authorized personnel and another that no weapons may be brought into the building. An access control system implements the first policy by requiring that people wishing to enter present a smart card with a biometric that matches the stored biometric of the authorized person. A detection system implements the second policy by requiring people to pass through a metal detection portal and their belongings to be scanned by an x-ray machine. These procedures ensure compliance with the policies. However, to be effective, security personnel must enforce the policies by following the prescribed procedures. If security personnel allow exceptions to these procedures, they are failing to enforce compliance with the policies. Just as damaging is the lack of effective security processes. For example, if there are no processes in place to handle the entry of employees who have forgotten their special identity cards, a vulnerability may be created that could be exploited by adversaries.

Breaches in security resulting from human error are more likely to occur if personnel do not understand the risks and the policies that are put in place to mitigate them. Good training is essential to successfully implementing policies by ensuring that personnel exercise good judgment in following security procedures. In addition, having the best available security technology cannot ensure protection if people have not been trained in how to use it properly. Good training is particularly essential if the technology requires personnel to master certain knowledge and skills to operate it. For example, x-ray inspection systems rely heavily on the operator to detect concealed objects in the generated x-ray images. If security personnel have not received adequate training in understanding how the technology works and making them adept at detecting threat images, such as a knife, the security system will be much less effective.

The Capabilities of Security Technologies Can Be Overestimated

It is also important to determine how effective technologies really are. Are they actually as accurate as vendors state? In overestimating their capabilities, security officials risk falling into a false sense of security and relaxing their vigilance.

During our review, we found instances in which the performance estimates vendors provided for some of their biometric technologies were far more impressive than those obtained through independent testing. As always, it is important to keep in mind the adage of "buyer beware" when making procurement decisions. There are publicly available resources that provide assessment guidance regarding security products. For example, the National Institute of Justice has evaluated a number of security products over the past few years and can serve as a valuable resource to federal agencies for making purchasing decisions (see http://www.ojp.usdoj.gov/nij/about_sci.htm).

Also bear in mind that lower technological solutions sometimes may be more effective and less costly than more advanced technologies. Dogs, for example, are an effective and time-proven tool for detecting concealed explosives. The dogs currently used in DoD, for example, can detect nine different types of explosive materials. And since dogs have the advantage of being mobile and able follow a scent to its source, they have significant advantages over mechanical explosive detection systems in any application that involves a search.

The Involvement of Multiple Government Entities Is Required to Secure Federal Facilities

Technologies are countermeasures identified in the final step of the risk management process. As such, they are only capable of defending against recognized threats. If unrecognized threats are not factored into the risk management process, these risks will not be mitigated and the technologies that have been implemented may be ineffectual in preparing for them.

Security managers of federal buildings rely on federal, state, and local government entities to prevent, detect, and respond to acts of terrorism against their facilities. Because they are not aware of potential threats posed by foreign and domestic terrorist groups, federal security managers depend on intelligence and law enforcement agencies such as the Central Intelligence Agency, the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research to gather information about and assess such threats against their facility.

Security managers of federal buildings also do not have access to the range of emergency resources required to respond to terrorist attacks. They rely on state and local governments to provide fire-fighting, medical personnel, and other emergency services. They also rely on the police and the judicial systems to enforce and prosecute violators of the laws and regulations governing the protection of federal buildings.

TECHNICAL LIMITATIONS AND USER RESISTANCE POSE CHALLENGES TO IMPLEMENTATION

Despite significant advances in performance and capability, the newer security technologies still face considerable technical challenges and user acceptance issues before they can be effectively integrated and widely deployed in federal facilities.

The Lack of Standards Impedes System Integration

First, because there are no industrywide common standards for data exchange and application programming interfaces[7] for technologies that provide physical security, most of the equipment used by the technologies in our review is not interoperable. For example, deploying an access control system that uses a smart card containing a fingerprint biometric would require at least three pieces of equipment: the card reader device, the fingerprint scan device, and the hardware device used to house and operate the biometric software. If these devices are made by different manufacturers, they cannot function as an integrated environment without middleware to connect the disparate components. Not only does developing the initial customized middleware represent substantial expenditures, but new middleware will have to be developed whenever old equipment is replaced by equipment from a different manufacturer. Moreover, standardizing on one manufacturer's equipment is not the most advantageous option since doing so leaves no range of equipment from which to choose and requires replacing all existing hardware not made by that manufacturer. Although efforts are underway to address the problem of standards, it will be some time before this problem is resolved.

The Use of Several Security Technologies Continues to Generate Concerns about their Potential Violation of Expectations of Privacy

Second, Americans, as a society, expect and cherish the value and freedom of privacy. Recent concern within Congress and public interest groups alike about the intended use of CCTV by D.C. law enforcement agencies has highlighted issues regarding the consequences of the applications of newer security technologies on privacy.[8] In general, apprehensions are based on a fear of misuse, i.e., that these security technologies will be used for purposes other than for which they were intended. For example, there is a fear that the government may use the newer surveillance technologies to track people. Employees also fear that management will be tempted to monitor their performance. Also at issue is whether people will be arbitrarily monitored based on their race or ethnic origin or whether operators may be tempted to indulge in video voyeurism by, for example, especially focusing on young, attractive females.

There is also a concern that biometric technologies may reveal confidential medical information. Because diseases such as AIDS, diabetes, and high blood pressure cause changes to the retina, some people fear, for example, that retinal scans could compromise the privacy of this information.

---

[7] The interface between the application software and the application platform (i.e., operating system), across which all services are provided.

[8] The House Committee on Government Reform, Subcommittee on the District of Columbia held a hearing on the expanding use of electronic surveillance in the District of Columbia on March 22, 2001. During the hearing, the chairwoman and ranking minority member of the subcommittee emphasized the need for policies, procedures, and guidance to govern the use of CCTV technology because of the potential infringement on the public's privacy rights.

Civil liberties advocates also find the newer detection system technologies too intrusive. The tremendous potential for embarrassment was recently pointed out by newspapers reporting on low-dose x-ray systems installed at Orlando International Airport that essentially perform "virtual strip searches." These systems, now in a test phase, can see a person's body through clothing. Newspapers published pictures revealing images of a person's body – every inch of it – graphically captured by the scanner.

Not All Security Technologies Are User Friendly

Third, several of the security technologies we reviewed have the disadvantage of being both complex and inconvenient to use, requiring considerable user cooperation. Most biomctric technologies, in particular, have some negative features. Retina scanning, for example, feels physically intrusive to some users because it requires close proximity with the retinal reading device. And fingerprinting feels socially intrusive to some users because of its association with the processing of criminals.

There is also an assortment of health concerns among a segment of the population regarding certain security technologies. There is evidence that pacemakers and hearing aids can be adversely affected by some detection technologies. However, up until now no evidence has been produced to substantiate fears of radiation exposure from x-ray systems and apprehensions that certain detection systems could cause depression or even brain tumors. Certain groups of individuals resist using biometric devices because of hygiene issues.

In conclusion, our review has identified myriad commercially available technologies that implement the three essential concepts of effective security: protection, detection, and reaction. Many of these technologies are mature and have already been deployed in various federal facilities, where their capabilities and effectiveness have been demonstrated. Other newer technologies appear to offer great potential in helping federal agencies to ensure the security of their facilities. These technologies could be adopted in the near future. Other technologies are still in a nascent stage of development, but are maturing and appear promising. Many biometric technologies still face barriers in intrusiveness and complexity that must be addressed before they can be most effectively deployed and widely accepted by users. However, they offer greater security, and the challenges to their implementation may not be formidable.

However, of foremost importance is to continuously bear in mind that effective security can never be achieved by relying on technology alone. People will

always play a fundamental role in all phases: from planning to implementation and to enforcement. Accordingly, technology and people must work together as part of an overall security process, beginning with a risk management approach and incorporating, implementing, and reinforcing those three essential concepts.

Mr. Chairman and members of the subcommittee, this concludes my statement. I would be pleased to answer any questions you or the members of the subcommittee may have.

Contacts and Acknowledgment

For further information, please contact me at (202) 512-6412 or via e-mail at rhodesk@gao.gov. Individuals making key contributions to this testimony included Sophia Harrison, Ashfaq Huda, Richard Hung, Elizabeth Johnston, and Tracy Pierson.

Attachment I: Access Control Technologies

The first line of security within a federal building is to channel all access through entry control points where identity verification devices can be used for screening. These devices "authenticate" individuals seeking entry, i.e., they verify that the individuals are indeed authorized to be there by electronically examining credentials or proofs of identity.

Identity verification devices use three basic technological approaches to security based on something you have, something you know, and something you are. Accordingly, they range from automatic readers of special identification cards (something you have), to keypad entry devices that generally require a pin number or password (something you know), to more sophisticated systems that use biometrics (something you are) to verify the identity of persons seeking to enter a facility. More secure access control systems use a combination of several of these approaches at the same time for additional security.

Biometric Access Controls

The term "biometrics" covers a wide range of technologies used to measure and analyze human characteristics to verify a person's identity. Identifiable physiological characteristics include fingerprints, eye retinas and irises, and hand and facial geometry. Identifiable behavioral characteristics are speech and signature. Biometrics represents a theoretically very effective security approach because these characteristics are distinct to each individual and, unlike identification cards and pin numbers or passwords, they cannot be easily lost, stolen, or guessed.

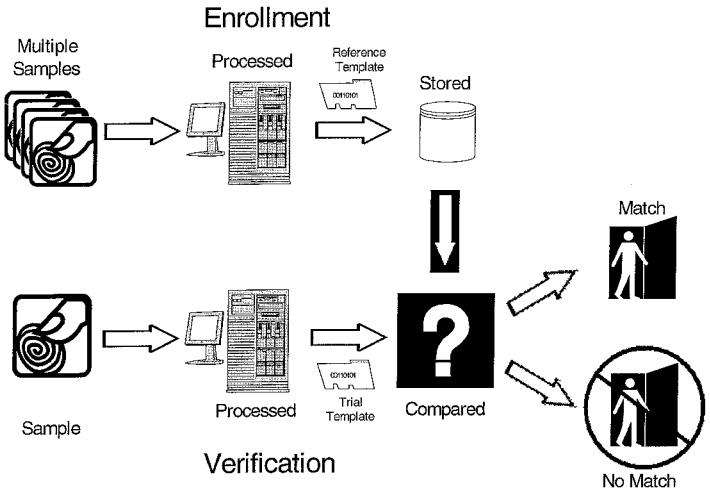


Figure 2: Biometric Identification Verification Process

Although biometric technologies measure different characteristics, all biometric access control technologies involve a similar process that includes the following components:

- Enrollment: multiple samples of an individual's biometric are captured (as an image or a recording) via an acquisition device (e.g., a scanner or a camera).
- Reference template: the captured samples are averaged and processed to generate a unique digital representation of the characteristic, which is stored for future comparisons. Templates are essentially binary number sequences. The size of the template depends on the technology, but generally ranges from 10 to 20,000 bytes. It is impossible to recreate the sample, such as a fingerprint, from the template. Templates can be stored centrally on a computer database, within the device itself, or on a smart card.

- Verification: a sample of the biometric of the person seeking access to a building is captured at the entry control point, processed into a trial template, and compared with the stored reference template to determine if they match.[9] Because the reference template is generated from multiple samples at enrollment, the match is never perfect. Therefore, systems are configured to verify the identity of users if the match exceeds an acceptable threshold.

The effectiveness of biometric systems is characterized by two error statistics: false rejection rates (FRRs) and false acceptance rates (FARs). For each FRR there is a corresponding FAR. A false reject occurs when a system rejects a valid identity; a false accept occurs when a system incorrectly accepts an identity. If biometric systems were perfect, both error rates would be zero. However, all biometric technologies suffer FRRs and FARs that vary according to the individual technology and its stage of development.

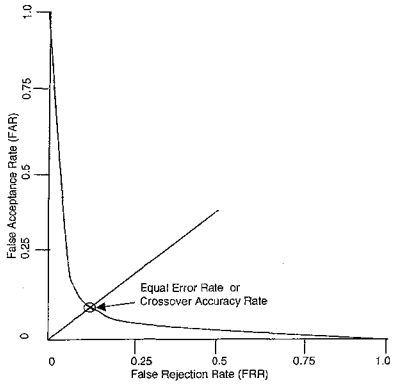
Because biometric access control systems are not capable of verifying identities with 100 percent accuracy, trade-offs must be considered during the final step of the risk management process when deciding on the appropriate level of security to establish. These trade-offs have to balance acceptable risk levels with the disadvantages of user inconvenience. For example, perfect security would require denying access to everyone. Conversely, granting access to everyone would result in denying access to no one. Obviously neither of these extremes is reasonable, and access control systems must operate somewhere between the two. How much risk one is willing to accommodate is the overriding factor in adjusting the threshold, which translates into determining the acceptable FAR. The tighter the security required, the lower the tolerable FAR.

Vendors of biometric systems are currently claiming that false accepts occur once out of every 100,000 attempted entries and that the FRR is about 2 to 3 percent. However, because system thresholds are adjusted to accommodate different FARs, it is often difficult to measure and compare their effectiveness. Vendors also describe the accuracy of their systems in terms of an equal error rate, also referred to as the crossover accuracy rate, or the point where the FAR equals the FRR.

---

[9]Unlike other access control systems, biometric systems can also identify an authorized user without the user having to present any other identifier, such as an identity card or a pin number or password, by looking through an entire database of authorized users to attempt to find a match. Whereas verification systems attempt to perform one-to -one matches, identification systems attempt to perform one-to-many matches. Systems operating in this mode naturally take longer; the bigger the database, the slower the search. They are also less accurate.

Figure 3: General Relationship between the FAR and FRR



Source: General Accounting Office

As shown, selecting a lower FAR increases the FRR--the chance that an authorized person will be denied access to a facility. Perfect security would require denying access to everyone. In this extreme case, the FAR would be "0" and the FRR "1." Conversely, granting access to everyone would result in a FRR of "0" and a FAR of "1."

Attachment I to be inserted here.

Attachment II: Detection Technologies

Detection systems provide a second layer of security. X-ray machines, metal detectors, and explosive detectors can be strategically deployed at entry control points to screen individuals and their belongings for hidden firearms, explosives, and other potentially injurious objects as they clear the access control system.

Attachment II to be inserted here.

Attachment III: Intrusion Detection Technologies

Intrusion detection systems serve to alert security staff to react to potential security incidents. These systems are designed to identify penetrations into buildings through vulnerable perimeter barriers such as doors, windows, roofs, and walls. These systems use highly sensitive sensors that can detect an unauthorized entry or attempted entry through the phenomena of motion, vibrations, heat, or sound.

Closed circuit television (CCTV) is an integral part of intrusion detection systems. These systems enable security personnel to monitor activity throughout a building. Intrusion detection technologies can also be interfaced with the CCTV system to alert security staff to potential incidents requiring monitoring.

When an intrusion is sensed, a control panel to which the sensors are connected transmits a signal to a central response area, which is continually monitored by security personnel. The sensor-detected incident will alert security personnel of the incident and where it is occurring. By interfacing these technologies, security personnel can initially assess sensor-detected security events before determining how to react appropriately.

Attachment III to be inserted here.

Mr. TOM DAVIS OF VIRGINIA. Our mystery as to where Mr. Turner is has been solved. He has been on the floor arguing an amendment. So he has an excused absence until he gets here.

Mr. Moravec.

Mr. MORAVEC. Good afternoon, Mr. Chairman, and members of the subcommittee.

I am Joe Moravec, Commissioner of the Public Buildings Service [PBS] at the General Services Administration [GSA]. I am pleased to appear before you today to provide information on GSA's program to secure Federal buildings that it owns or leases with a focus on the technologies necessary to achieve GSA's security objectives.

The mission of GSA's Public Buildings Service is to provide a superior workplace for the Federal worker and, at the same time, superior value for the American taxpayer. We design, build, and manage about 340 million square feet of work space for over a million Federal associates in about 8,000 buildings in 1,600 American communities across the country.

PBS's Federal Protective Service [FPS] provides security and law enforcement services for all of the buildings we own and lease. Our security philosophy is based on the premise that each facility presents a unique set of security and safety challenges. The mission of the Federal Protective Service is to enable Federal agencies and members of the public to conduct their business in a safe and secure environment.

FPS is comprised of Police Officers, Criminal Investigators, Physical Security Specialists and Contract Guards. We work collaboratively with Federal customers across the Nation to ensure that effective security procedures are in place for the safety of all occupants in and visitors to GSA-controlled facilities. We work to identify and reduce the threat to Federal property through the application of a program that employs law enforcement, criminal intelligence gathering and sophisticated countermeasures.

I prepared detailed answers to each of the questions to your letter of invitation, and I would like to submit them for the record. Let me summarize the theme of the responses.

Since September 11th, our security needs and response to threats have changed. Prior to September 11th, our greatest threat was perceived to be a vehicular bomb that could result, as in the case of Oklahoma City, in the total collapse of a building. September 11th made us realize that the universe of threats we face has expanded and the mentality of those who wish to do us harm is even more dangerous than we'd imagined. We now must be prepared not only for truck bombs but also for chemical and biological weapons and weapons of mass destruction delivered by individuals who have no regard for human lives, including their own.

In response to this, we have enhanced a number of efforts to protect our properties and the people housed in them. First, foreknowledge—knowledge of an imminent threat—is the best security measure. We are now working with the FBI, CIA and State and local law enforcement agencies in sharing of intelligence information that enables us to better assess the credibility of threats.

We have expanded our training and physical security, ensuring that our security professionals are trained and kept current in the

latest technologies and have access to the necessary intelligence information needed to develop specific countermeasures tailored to each facility. Each facility in the tenant agency operation is analyzed individually. Countermeasures are now building specific.

We have also increased our ability to assess the effectiveness of a range of countermeasures that include building design modifications, site modifications, increased guard services and new technologies. Our threat assessment methodology for each building enables us to create a set of countermeasures designed to reduce the threat at that building.

We also have increased our outreach to our Federal agency customers and to our GSA associates. They are our eyes and ears in the counterterrorism campaign. We conduct awareness briefings, have distributed pamphlets on keeping our building safe and on how to respond to suspicious acts. Our customers and associates have become vital and vocal members of each Building Security Committee.

Finally, we know that processes and technologies are only as good as the people who follow or use them. We must maintain a well-trained and experienced law enforcement work force. We are exploring legislative and administrative options to help ensure we will continue to have a well-trained and stable work force capable of providing the necessary level of security needed to protect our facilities.

Our goal is the safety and security for everyone in GSA-controlled space. We can only accomplish this goal through the use of technology, deployment of trained law enforcement professionals and contract guards, partnering with our fellow Federal, State and local law enforcement agencies and, perhaps most importantly, by encouraging all our associates to move to a higher sustainable level of alert, awareness and vigilance. Combining all of these will ensure that we can achieve a proper balance of openness and security in Federal facilities across the Nation.

This concludes my prepared statement, Mr. Chairman. I have attached my statement and answers to issues raised by the subcommittee. I will be pleased to answer any questions that you or other members of the subcommittee may have on this matter.

[The prepared statement of Mr. Moravec follows:]

STATEMENT

OF

F. JOSEPH MORAVEC

COMMISSIONER

OF THE

PUBLIC BUILDINGS SERVICE

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

APRIL 25, 2002

Good afternoon Mr. Chairman, and members of the Subcommittee. I am F. Joseph Moravec, Commissioner of the Public Buildings Service (PBS). I am pleased to appear before you today to provide information on the General Services Administration's (GSA's) program to secure the Federal buildings that it owns or leases with a focus on the technologies necessary to achieve GSA's security objectives.

The mission of GSA's Public Buildings Service is to provide a superior workplace for the Federal worker and at the same time superior value for the American taxpayer. We design, build and manage about 340 million square feet of workspace for over a million Federal associates in about 8,000 buildings in 1,600 American communities across the country.

PBS' Federal Protective Service (FPS) provides security and law enforcement services for all of the buildings we own and lease. Our security philosophy is based on the premise that each facility presents a unique set of security and safety challenges. The mission of the FPS is to enable Federal agencies and members of the public to conduct their business in a safe and secure environment. FPS is comprised of Police Officers, Criminal Investigators, Physical Security Specialists, and contract guards. We work collaboratively with Federal customers across the nation to ensure that effective security procedures are in place for the safety of all occupants in and visitors to GSA-controlled facilities. We work to identify and reduce the threat to Federal property through the application of a program that employs law enforcement, criminal intelligence gathering and sophisticated countermeasures.

I have prepared detailed answers to each of the questions in your letter of invitation, and would like to submit them for the record. Let me, however, summarize the theme of the responses.

Since September 11, 2001, our security needs and response to threats have changed. Prior to September 11th, our greatest threat was perceived to be a vehicular bomb that could result - as in the case of Oklahoma City - in the total collapse of a building. September 11th made us realize that the universe of threats we face has expanded, and the mentality of those who wish to do harm is even more dangerous than we imagined. We now must be prepared not only for truck bombs, but also chemical and biological weapons and weapons of mass destruction delivered by individuals who have no regard for human lives, including their own.

In response to this, we have enhanced a number of efforts to protect our properties and the people housed in them. First, foreknowledge - knowledge of an imminent threat - is the best security measure. We are now working with the FBI, CIA and State and local law enforcement agencies, in the sharing of intelligence information that enables us to better assess the credibility of threats.

We have expanded our training in physical security, ensuring that our security professionals are trained and kept current in the latest technologies and have access to the necessary intelligence information needed to develop specific countermeasures tailored to each facility. Each facility and the tenant agency operation is analyzed individually. Countermeasures are now building specific.

We have also increased our ability to assess the effectiveness of a range of countermeasures that include building design modifications, site modifications, increased guard service and new technologies. Our threat assessment methodology for each building enables us to create a set of countermeasures designed to reduce the threat at that building. We also have increased our outreach to our Federal agency customers and to our GSA associates. They are our eyes and ears in the counter terrorism campaign. We conduct awareness briefings, have distributed pamphlets on keeping our buildings safe and on how to respond to suspicious acts. Our customers and associates have become vital and vocal members of each Building Security Committee.

Finally, we know that processes and technologies are only as good as the people who follow or use them. We must maintain a well-trained and experienced law enforcement workforce. We are exploring legislative and administrative options to help ensure we will continue to have a well-trained and stable workforce capable of providing the necessary level of security needed to protect our facilities.

Our goal is the safety and security for everyone in GSA-controlled space. We can only accomplish this goal through the use of technology, deployment of trained law enforcement professionals and contract guards, partnering with our fellow Federal, State and local law enforcement agencies and, perhaps most importantly, by encouraging all of our associates to move to a higher sustainable level of awareness and vigilance. Combining all of these will ensure that we can achieve a proper balance of openness and security in Federal facilities across the nation.

This concludes my prepared statement Mr. Chairman. I have attached to my statement answers to issues raised by the Subcommittee. I will be pleased to answer any questions you or the other members of the Subcommittee may have on this matter.

House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
Oversight Hearing
Rayburn Building, April 25th at 2 p.m., Room 2154

Issue 1: What does GSA consider the acceptable minimum level of security in a Federal building? What factors are considered in making this determination?

Answer: Above all, the only acceptable minimum-security level for all of our facilities is that which provides for a safe and secure environment for our GSA co-workers, customers, and visitors. This is the driving force behind our mission: to permit Federal agencies and members of the public to conduct their business without fear of violence, crime, or disorder.

The factors that we rely upon to establish and maintain this level of security are derived from two principal sources. The first source is actually two publications - the 1995 Department of Justice Vulnerability Assessment of Federal Facilities Report (the 1995 DOJ Report), and the 2000 Interagency Security Committee Security Design Criteria for New Federal Office Buildings and Major Modernization Projects (ISC Security Design Criteria). These two publications provide recommendations and guidelines for minimum-security standards and form the baseline that GSA uses when determining security standards.

The second source is the Building Security Assessment (BSA) program developed by the Public Buildings Service's Federal Protective Service to determine the specific building security measures needed for each building to eliminate or reduce threats directly associated with the building. In conducting a security assessment, factors such as: the facility's unique features and existing countermeasures, identification of credible threats, determination of risk level for each threat, determination of acceptability of certain risks, identification of countermeasure upgrades, and reassessment of risk level after new countermeasures are implemented – are used to ultimately reach the optimum security level for each building.

House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
Oversight Hearing
Rayburn Building, April 25th at 2 p.m., Room 2154

Issue 2: What technologies are critical to achieving the minimum-security standards? Are these technologies cost-prohibitive?

Answer: As explained in our answer to question number 1, we address each building on a case-by-case basis to make certain the highest level of security is achieved for each building. In turn, the technologies critical to achieving minimum-security standards for a building are designed specifically for that building.

For new buildings this process will begin with the actual design of the building itself to ensure all aspects of the building are considered. This would include such items as construction provisions to address progressive collapse, window/glass protection, building setback, HVAC protection, and a comprehensive perimeter security system.

GSA refers to the ISC Security Design Criteria as a guideline for all new Federal buildings and existing Federal buildings that are undergoing major modernization.

For existing Federal buildings, GSA refers to the 1995 DOJ Report for minimum-security standards. To assist us in developing the building specific security systems, PBS's Federal Protective Service security professionals conduct BSAs on each GSA-controlled building. The BSAs determine existing and/or potential credible threats to a building. While the ISC Security Design Criteria and the 1995 DOJ Report are used as guidelines for building minimum-security standards, the BSAs will ultimately determine the specific security measures needed for each building to achieve the highest possible level of security.

The technologies currently being used in GSA buildings are singularly not cost prohibitive. However, when you factor in the building design features such as progressive collapse and window/glass protection with the overall security system features, the costs incurred can be high. Price, including life cycle and training costs, is not the deciding factor. Effectiveness is the most determining factor.

Below are the most common security technologies or equipment employed as countermeasures:

- Security Lighting
- Barriers – Physical and Vehicle, high security locks
- Closed Circuit TV
- Security Systems- intrusion detection/fire systems, etc. with Central Station Monitoring
- Uninterruptable Power Supply
- Photo Identification
- Visitor Control
- Security guards
- X-ray Machines

House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
Oversight Hearing
Rayburn Building, April 25th at 2 p.m., Room 2154

Answer 2 – Continued:

- Magnetometers
- Explosive detection systems, hand held units, mobile units, canine
- Under Vehicle Inspection System
- Air in-take, HVAC protection
- Backups for critical infrastructure components (radio communications/computer facilities)

House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
Oversight Hearing
Rayburn Building, April 25th at 2 p.m., Room 2154

Issue 3: How does GSA assess the effectiveness of its security measures?

Answer: Since the September 11, 2001 attacks, GSA has moved to a proactive posture by focusing on identifying the threat to our customers and measuring the reduction of threat. GSA's FPS is now actively involved in various Federal intelligence groups such as the FBI's Joint Terrorism Task Force and the CIA's Interagency Intelligence Committee on Terrorism, and has moved from a patrol and response mode to assessing the risks and employing countermeasures before incidents occur. A major lesson learned from the Oklahoma City bombing is that we cannot address security in broad terms. We must rely on unique assessments of each building.

GSA, through its Office of Federal Protective Service, recently developed a Regional Threat Assessment (RTA) program to capture the major threats to the Federal workplace. It gives decision-makers a tool to put efforts and resources in priority order. The RTA, an internal management tool, examines criminal intelligence, risk management assessments, security perceptions, and other factors to identify the major threat(s) to a GSA Region. An RTA is also an outcome performance measure that quantifies the efficiency of a GSA Region in reducing the threat.

We are also developing the strengths of our personnel, harnessing technology to support our effectiveness, and measuring our performance. Throughout the process, we concentrate on maintaining consistency in the methods we use to deliver our protection services.

In addition to the RTA and Building Security Assessment processes, GSA is constantly receiving feedback on our service through customer satisfaction surveys. These surveys provide GSA with vital information on our facilities from our tenants' perspective. Specifically, how they rate the security measures in place in their buildings. Additionally, each GSA controlled building is required to have a Building Security Committee, which is charged with overseeing security matters within their building. The committee is made up of a representative from each tenant agency and chaired by the agency with the largest population. FPS personnel are the principal security consultants to the Building Security Committees and provide valuable input on the effectiveness of security in their buildings.

House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
Oversight Hearing
Rayburn Building, April 25th at 2 p.m., Room 2154

Issue 4: How does GSA balance the implementation of security standards with convenience and Federal employees' privacy?

Answer: Security is of paramount concern to GSA, yet we are sensitive to the overall needs of our customers. We want to create an environment within our buildings that reflects an open welcome atmosphere, but one that challenges those with intent to do harm. Our goal is aesthetically pleasing facilities with optimum security that allows Federal agencies and members of the public to conduct their business without fear of violence, crime, or disorder.

To obtain a balance between the Federal workers' convenience and privacy and the inclusion of minimum-security standards in a building, GSA encourages close coordination between its security, engineering, architectural, and design associates. Extensive discussions are held with building occupants to determine specific agency needs and to apprise them of GSA's efforts to enhance their safety, as well as the safety of the building. GSA also reaches out to private sector building design and architectural professionals to accomplish our goal of creating a welcoming and secure environment.

There are times, however, when security may overrule employee convenience and privacy. As an example, immediately following the attacks on September 11, 2001, additional security measures were instituted at all of our buildings – most with little, if any, advanced warning to building occupants.

As a means to ease this intrusion, building occupants were advised of the added security measures as soon as possible. As the likelihood of additional attacks decreased, the security measures were decreased accordingly. In the wake of the anthrax attacks, GSA again needed to increase its security measures quickly and relied heavily upon our building occupants' patience in dealing with this threat.

To help educate and assist our building occupants nationwide, GSA published a pamphlet, "Making Federal Buildings Safe", and distributed the pamphlet throughout our buildings. We have also provided emergency planning information on our web site so that the information is readily available to our associates and customers. We have found that the combination of strong internal GSA coordination and open communication with our building occupants has helped us maintain an acceptable balance between implementation of building security standards and Federal employees' convenience and privacy.

House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
Oversight Hearing
Rayburn Building, April 25th at 2 p.m., Room 2154

Issue 5: What are some of the challenges posed by the variety of real estate arrangements GSA has made for agencies? For example, if an agency leases one floor, or even part of a floor, in a privately owned building can GSA guarantee the security of that space? If there are restrictions in the lease agreement, what alternatives exist for securing these sites?

Answer: It is our goal, yet our biggest challenge, to provide the same level of security for the occupants of our leased facilities as we have for those in the buildings that we own. It is much easier for GSA to address security in the buildings we own due to our ability to make whatever changes needed to facilities – many times on short notice. It is much different in our leased facilities due to our need to work with landlords and their buildings; and, in some instances, to coordinate with the needs and expectations of the building's other non- Federal tenants.

GSA Portfolio Management and Federal Protective Service personnel work with the landlords to define a proper security plan for our customers. For existing leased space the minimum-security standards recommended in the 1995 DOJ Report are followed as closely as possible. For leased space to be constructed, GSA follows closely the security standards established in the ISC Security Design Criteria. In some cases in a lease space where we modify the space for our customer, the space must be restored to its original condition before returning the property to the landlord. Any duty to restore the premises should be established with our customers at the inception of the lease and should be reflected in GSA's Occupancy Agreement with the Federal agency tenant. At times, such as immediately following the September 11, 2001 attacks, GSA must implement security measures in our leased spaces even over the objections of the landlord. Those instances are relatively rare and are only done so when absolutely required.

When there are restrictions in a lease agreement that make it unreasonable for GSA to implement appropriate security measures, GSA will seek alternative means to ensure the security and safety of the agency's associates, including possibly relocating the agency.

House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
Oversight Hearing
Rayburn Building, April 25th at 2 p.m., Room 2154

Issue 6: In the wake of the terrorist attacks on September 11, what new security needs have been identified?

Answer: The most important security consideration identified since September 11th, is the realization that we are now dealing with a completely different terrorist mindset. We have realized that the modern day terrorist will do whatever it takes to accomplish his objective whether it is through the use of planes, the U.S. mail, or weapons of mass destruction. Therefore, our approach to security can no longer be based on a broad-brush, across-the-board, solution. Since our security needs must now address specific threats, we have joined with other Federal and local law enforcement organizations and intelligence agencies to share the most accurate and up-to-date information available. This information must include both domestic and international terrorist and criminal developments. We are exploring legislative and administrative options to enhance the operational capability of the Federal Protective Service.

Since the September 11th attacks, we have seen an increase in requests for implementation of additional countermeasures at our buildings. The type of countermeasures recommended and requested since the terrorist attacks have been geared toward items such as: explosive detection systems, under vehicle inspections, air intake sensors, bomb dogs, and biological/chemical detection equipment. Based on the type of threat identified at a building and/or at the request of a Building Security Committee or client agency, GSA has purchased and implemented many of these countermeasures.

House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
Oversight Hearing
Rayburn Building, April 25th at 2 p.m., Room 2154

Issue 7: After September 11, there was an immediate demand and response for increased security in Federal buildings. Has GSA managed to ensure cost-efficiency while obtaining effective new technologies to address the new security threats?

Answer: We are actively managing cost-efficiency in a variety of ways. We continually evaluate new equipment as it is introduced in the market place to determine its applicability to locations that are owned or leased by the General Services Administration. In this regard we are forming a group of in-house security managers to review and test equipment that we could use in our countermeasure programs. We actively work with the American Society for Industrial Security to explore new ideas and technologies. Further, we have done a great deal of research with government and private organizations to develop new construction methods and standards for use as we design and build new Federal buildings.

We serve as the chair for the Interagency Security Committee which is a group made up of security managers from most government agencies and a focal point to evaluate all types of security needs and potential solutions.

When developing the appropriate level of countermeasures, we use all available research on equipment advances and construction methodologies. As a cost saving measure we have developed national multiple award contracts to achieve economies of scales and volume discounts. In addition to GSA's purchases, other government agencies are able to use these contracts to purchase security devices directly from the vendors, which in turn, allows GSA to negotiate the most favorable prices. We continually review these contracts as new equipment comes available that may provide better or equal services at reduced costs. Much like the computer industry did just a few years ago, the security equipment industry is developing new and improved equipment at better prices. Balancing the necessary equipment with the best price is a daily part of our mission to the taxpayer and our tenants.

Mr. TOM DAVIS OF VIRGINIA. I think we will continue and probably can get a couple more testimonies before we go over to vote. Mr. Jester.

Mr. JESTER. Thank you, Mr. Chairman. Thank you for this opportunity to report to you on the Department of Defense's efforts to secure its federally owned and leased office buildings.

As the Chief of the Defense Protective Service, I manage an organization responsible for providing force protection, security and law enforcement for the employees, facilities, infrastructure and other sources at the Pentagon and other DOD-occupied buildings in the national capital region.

Although there are considerable challenges, I am pleased to report that we have made tremendous progress before and after the September 11th terrorist attacks. Moving beyond traditional guard forces and electronic alarm systems, we are executing a comprehensive force protection program that will provide enhanced protection for DOD employees, property and operations occupying leased and owned facilities. Leased facilities do present unique challenges for security. However, we are making every effort to ensure the safety and security of DOD agencies in leased buildings.

In addition to the basic technologies that have been used to control access and detect explosives, we are beginning to use existing and new technology in several areas, notably in our chemical, biological and radiological program.

While technology is providing many tools to augment our security forces, we have not forgotten security principles such an emergency planning, exercises and drills and work force awareness. These basic measures were critical components in our response to the terrorist attack at the Pentagon.

I prepared specific written responses to your questions submitted to me and submitted those to your staff.

That concludes my written response. Thank you.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Jester follows:]

Testimony of John N. Jester
Department of Defense

Mr. Chairman and distinguished members of the subcommittee, thank you for this opportunity to report to you on the Department of Defense's efforts to secure its' federally owned and leased office buildings.

As the Chief of the Defense Protective Service, I manage an organization responsible for providing force protection, security and law enforcement for the employees, facilities, infrastructure and other sources at the Pentagon and other DoD occupied buildings in the National Capital Region.

Although there are considerable challenges, I am pleased to report that we have made tremendous progress before and after the September 11th terrorist attack. Moving beyond traditional guard forces and electronic alarm systems, we are executing a comprehensive force protection program that will provide enhanced protections for DoD employees, property and operations occupying leased and owned facilities. Leased facilities do present unique challenges for security: however, we are making every effort to ensure the safety and security of DoD agencies in leased buildings.

In addition to the basic technologies that have been used to control access and detect explosive, we are beginning to use existing and new technology in several areas, notably in our chemical, biological and radiology program.

While technology is providing many tools to augment our security forces, we have not forgotten basic security principles such as emergency planning, exercises and drills and workforce awareness. These basic measures were critical components in our response to the terrorist attack at the Pentagon.

In response to the specific questions submitted to me by your staff, I have prepared a written response and submitted it to your staff. I will be happy to answer any questions you have on this important subject.

Department of Defense Response

1. What does DOD consider the acceptable minimum level of security in a federal building? What factors are considered in making this determination?

DoD Regulation 5200.8-R, Physical Security Program, prescribes standards and policy for security of DoD assets. Additionally, DoD Instruction 2000.16, DoD Antiterrorism Standards, establishes 31 minimum defensive measures to reduce the vulnerability of individuals and property to terrorist acts.

Minimum levels of security for specific facilities are developed using a risk management approach. The analytical process includes defining assets, the threats against them, and their vulnerabilities.

One key element we consider in determining an acceptable level of security is the ability to maintain a controlled environment for the DoD operations in the building.

2. What technologies are critical to achieving the basic security measures?

Critical technologies include electronic intrusion detection, access control, closed circuit television and explosive detection. We are now using and testing technology used to detect chemical, biological and radiological threats.

The September 11 attacks also proved the need for communication systems.

3. How does DOD assess the effectiveness of its security measures?

All facilities are subject to vulnerability assessments, conducted on a recurring basis by multidiscipline teams from the Defense Threat Reduction Agency, the military services and defense agencies. Specifically, Joint Staff Integrated Vulnerability Assessments highlight personnel and facility protection, while Balanced Survivability Assessments focus on the protection of critical infrastructures as they relate to mission assurance.

4. How does DOD balance the implementation of security measures with convenience and the privacy of federal employees' and visitors?

Convenience is often counter to good security practices. Our job requires that we not only design and implement security systems, but also explain that need to the workforce to be security conscious and practice security in their daily activities.

Our security measures are focused on public areas where there is no expectation of privacy. We do not employ such measures as closed circuit television in offices or other areas where there is an expectation of privacy.

5. What are some of the challenges posed by the variety of DOD's real estate arrangements? For example, if DOD leases one floor, or even part of a floor, in a privately owned building can the agency guarantee the security of that space? If there are restrictions in the lease agreement, what alternatives exist for securing these sites?

One of the greatest challenges in leased facilities is working with uncooperative building owners that prevent the government from implementing security in their building. This is due in most cases to the fact that the required security measures were not clearly spelled out in the solicitation for leased space. It is extremely important for a government agency to clearly define their security requirements in the solicitation. If there are restrictions in a lease agreement, the first course of action is determine if the lessor will permit a modification to the lease. If not, a decision should be made to determine if the required security measures out weigh the need for the agency to remain in that particular building.

6. In the wake of the terrorist attacks on September 11, what new security needs have been identified?

Emerging needs include cost-effective countermeasures for chemical, biological and radiological threats. Additional resources are also necessary to mitigate traditional threats, principally from explosive devices. The need to project security measures further out from the building to the roads and grounds created a need for more police officers and guards.

7. After September 11, there was an immediate demand and response for increased security in federal buildings. Has DOD managed to ensure cost-efficiency while obtaining effective new technologies to address the new security threats?

We rely on inputs from two principal sources; the Physical Security Equipment Action Group (PSEAG), and the Technical Support Working Group (TSWG). Those groups conduct rapid prototyping and commercial off-the-shelf testing of equipment and systems. The TSWG has been effective in providing prototype equipment to the interagency community to combat terrorism. The PSEAG has been effective in making the latest technologies on physical security available to all of DoD. These two sources have assisted DoD in the application of cost efficient technology.

Mr. TOM DAVIS OF VIRGINIA. Mr. Abram.

Mr. ABRAM. Mr. Chairman and members of this subcommittee, thank you very much for inviting me to testify before you today on new surveillance technologies available to protect Federal buildings.

I am Frank Abram, General Manager of the Security and Vision Systems Group of Panasonic Digital Communications and Security Co., a leading supplier of security systems to both the U.S. Government and private industry.

The security industry landscape has changed dramatically over recent years. Technology has progressed more in the last 5 years than it has in previous decades. Categorically, the two product classifications showing the most significant growth are video surveillance and access control. Today, I would like to provide you with a brief overview of some of the new technologies and comment on how the security industry can work with the U.S. Government to implement them.

With the introduction of the first Digital Signal Processing cameras in the late 1980's, the performance of video surveillance took a quantum leap forward. Since then, video surveillance cameras have continued to evolve with each new generation.

Perhaps the most significant development in this area has been the introduction of Super Dynamic II technology. SDII provides a video acquisition method that most closely simulates how the human eye detects and processes light. This technology provides a cost-effective solution to one of the most prevalent problems facing video surveillance system designers and installers—extreme light contrast within a scene. Today, SDII cameras are employed in a number of high-profile government facilities such as our embassies and consulates and the Federal Aviation Administration simply because of their light-sensing capabilities.

New recording technology is also available. The proliferation of high-capacity hard drives has enabled video manufacturers to incorporate this reliable medium in a new generation of digital recorders specifically designed for security operations. In addition to their digital recording superiority, hard drive recorders incorporate numerous digital features that further enhance their utility beyond the traditional VCRs such as their ability to send images via the network.

One of the security industry's greatest challenges has long been personnel authentication, since traditional forms of identification and access control can easily be replicated loss or stolen. The introduction of easily deployed biometric systems are alleviating these problems, because biometrics are virtually impossible to replicate. This is particularly true of one of the newest biometric technologies, iris recognition.

Over the past year, iris recognition systems have become more affordable and practical for a wide range of access control and cyber security applications. These systems will provide added security with little or no inconvenience when entering a facility or accessing a computer terminal. With access control more of a concern than ever before, biometrics and iris recognition technology in particular can play an increasing role in homeland defense strategies.

I believe budget and education are the two most common factors that constrain security operations by government facilities. Additionally, security personnel in Federal agencies and in general find it difficult to keep pace with today's rapid development of new surveillance and security technologies. Manufacturers of surveillance and security systems equipment can help alleviate these constraints by providing more education opportunities through the government. By keeping government security personnel appraised of new technology developments, we can foster the intelligent deployment of new systems technology where it is most needed.

Another problem that has hampered the wide area of modernization of security in Federal buildings is the lack of set standards. One of the priorities for securing Federal buildings should be the establishment of a set of standards that clearly outlines the security measures to be taken. This will help assure minimal levels of security at each and every facility and bring attention to present deficits.

The standard should also include more thorough specifications to assure greater levels of performance, compatibility and future system expansion.

Thank you again for this opportunity to share with you my perspectives. I look forward to answering any questions you may have regarding security technologies or my comments on the way the Government may better secure its buildings.

[The prepared statement of Mr. Abram follows:]

STATEMENT OF FRANK ABRAM
GENERAL MANAGER, SECURITY AND VISION SYSTEMS GROUP
PANASONIC DIGITAL COMMUNICATIONS & SECURITY COMPANY

Before the
House Committee on Government Reform
Subcommittee on Technology and Procurement Policy
U.S. House of Representatives
Washington, DC

"Ensuring the Safety of our Federal Workforce: GSA's Use of Technology to Secure Federal Buildings"

April 25, 2002

Mr. Chairman and members of this subcommittee, thank you very much for inviting me to testify before you today on new video surveillance technologies available to protect Federal buildings. I am Frank Abram, General Manager of the Security and Vision Systems Group of Panasonic Digital Communications and Security Company. My over 27 years of experience in the CCTV and security market extends well beyond my career with Panasonic. I was first introduced to CCTV systems technology as a dealer, and then moved on to work for a major systems integrator.

My company is a leading marketer of closed circuit TV, video security and surveillance systems products, as well as other industrial and medical imaging products, professional audio and large screen display systems. It is a division company of Matsushita Electric Corporation of America, which is best known by its Panasonic brand name, and which markets a wide range of Panasonic consumer and industrial electronics products in the United States.

As a leading supplier of video surveillance technology, Panasonic video surveillance systems are presently employed in major facilities around the globe, including numerous installations in Federal Buildings and private industry here in the United States. I would be happy to provide you privately a list of those Federal agencies where we provide video surveillance systems. As a result of the company's expertise in the security field, Panasonic is considered an authoritative source for information, trends and new technologies that are shaping the security industry.

Introduction:
The security industry landscape has changed dramatically over recent years. The technology available today has progressed more in the last five years than it has in previous decades. As a result, there are many new technologies available with the potential to greatly enhance the safety and security of our Federal buildings and the personnel who occupy them. Categorically, the two product classifications showing the most significant growth are video surveillance and access control, due to an influx of new technologies that have greatly enhanced the coverage and control capabilities for advanced security systems applications. Today I want to provide you with a brief overview and understanding of the new security technologies being used for video surveillance and access control and to comment on how the security industry can work with the U.S. Government to ensure the availability and use of the most advanced technology for various security applications.

When considering how to most effectively secure Federal Buildings, it may be helpful to divide the areas of most concern into three zones of protection: Perimeter, parking areas/ access roads and interior. If you diagram these areas, you will see that they fall into concentric circles that require heightened security as you approach the innermost points. This model presents a clearer perspective on how security systems need to

increase in concentration as one gets closer to the access and egress points leading into a facility.

Each of the three zones of protection calls for specific security requirements that overlap to form a centralized security system. Perimeter protection should provide wide scale, overlapping coverage with cameras that offer zoom capability and the ability to adjust to changing lighting conditions. Additional considerations are low light level and infrared cameras to monitor dark recesses in the coverage areas. This will allow security personnel to detect potential problems or suspicious activities from a centralized location, and limit the deployment of personnel, which can cause deficiencies at primary locations within the facility.

Parking areas are a growing area of concern because of their proximity around or below a structure. Access and egress points should be protected by a combination of personnel, video surveillance cameras and some combination of authentication, including card/proximity readers, biometric devices and, of course, standard issued identification. A number of different camera technologies can be employed for indoor and outdoor parking areas to best suit specific lighting conditions.

The same authentication technologies might also be used for entry/egress to facilities, and as a means of controlling the accessibility to internal locations.
In addition to stationed security personnel and authentication systems, all entrance/egress points to a facility – lobbies, service entrances, drop points --should be continuously monitored by video surveillance cameras to provide images to a centralized monitoring station. It is also recommended that heavily traveled hallways, stairwells and other "public" areas be monitored with video surveillance cameras. Internal monitoring can take a more unobtrusive posture in an effort to preserve individuals' comfort levels and sense of privacy. Although cameras should be clearly visible, they need not be intrusive.

All of these measures will help provide security personnel with the information and extended presence to respond to suspicious activity and incidents in a fast and efficient manner. The visible presence of video surveillance and other security measures also provides a powerful deterrence factor, which can, in and of itself, thwart potential problems. As I mentioned, it is the advancement of video technology that has enabled the tremendous growth in available surveillance systems.

Technology Overview:
Video Surveillance - Cameras
With the introduction of the first Digital Signal Processing (DSP) cameras in the late eighties, patented by Panasonic's parent company Matsushita Electric, the performance of surveillance cameras took a quantum leap forward. Since then, video surveillance cameras have continued to steadily evolve with each new generation yielding higher levels of resolution, light sensitivity, color reproduction and reliability. Perhaps the most significant development in cameras has been the introduction of Super Dynamic II (SDII) technology.

SDII provides a video acquisition method that most closely simulates how the human eye detects and processes light. Combined with high resolution CCD image sensors and digital features that further enhance viewing operations, SDII cameras can effectively reduce the number of cameras formerly required to monitor a given location.

The most significant attribute of SDII technology is that it provides a cost-effective solution to one of the most prevalent problems faced by video surveillance system designers and installers -- extreme light contrast within a scene. A perfect example is a building lobby with windows and/or glass doors. The changing lighting conditions – from bright external sunlight to artificial internal lighting – cannot be simultaneously monitored by a single conventional camera. The only alternative previously available would be to utilize two cameras to monitor the same physical space. The Federal Aviation Administration headquarters here in Washington, D.C. is a prime example of how new camera technology can alleviate the need for redundant camera systems.

With SDII technology, video surveillance cameras now can capture highly viewable color and/or black-and-white images in areas where conventional cameras have previously been less efficient. A newly developed CCD and enhanced Digital Signal Processing (DSP) circuitry produce a dynamic range that is 32 times greater than conventional cameras. As a result, Super Dynamic cameras produce images that allow you to simultaneously view both the dark and bright areas of a scene -- with little or no picture loss. This unique capability makes Super Dynamic cameras ideal for many common applications where there are highly contrasted lighting conditions -- or for camera coverage in areas where lighting conditions change throughout the course of the day.

Super Dynamic cameras also incorporate a highly advanced image sensor that is radically different from conventional CCDs. In short, the new device reads and digitizes image signals at two different speeds -- short fast signals register bright image areas and long slower signals register dark image areas. The two signals are then processed together in the camera and combined into a single image. The resulting composite image displays both dark and bright areas without the need for frame memory, light compensation circuitry and masking techniques that simply block out bright areas.

Today DSP SDII is available in many different camera configurations – box cameras, unitized camera systems and most recently mini-dome vandal proof cameras.

Vandal proof mini-dome video surveillance cameras are available in indoor surface mount and flush mount configurations, as well as an outdoor weather resistant unit. The units incorporate a wide selection of performance benefits, such as SDII camera technology, to capture highly viewable color and/or black-and-white images under extreme lighting conditions within the same scene and Day/Night Operation that enable the cameras to switch from color to black and white according to the detected light levels.

Day/Night Operation automatically adjusts to changing light levels to provide color images in bright light (light levels as low as 1.6 lux), and highly detailed black and white images (as low as 0.2 lux) in dim lighting. More advanced Day/Night cameras also monitor RGB levels so they can adjust to the type of lighting available before making the transition from one mode to the other. The cameras' transition from color to black and white operation also can be programmed. In addition, the units are IR sensitive for use in virtual darkness. A variety of different camera models are available that feature this capability.

Video Surveillance - Hard Drive Recorders

The proliferation of high capacity hard drives has enabled video manufacturers to incorporate this reliable recording medium into a new generation of digital recorders specifically designed for security applications. In addition to their digital recording superiority, hard drive recorders incorporate a wealth of features that further enhance their utility in a security environment.

These features include on-board 10/100Base-T networking and motion detection features, as well as modular storage expansion up to 2 terabytes. To solve the archiving solution inherent with the technology, external and internal DVD-RAM and CD archiving solutions also are available that can play back recorded video directly from the DVD-RAM or CD in their native formats for added versatility, and without affecting hard drive capacity. With the addition of these archiving solutions, today's hard drive recorders can function as primary recorders in a video surveillance system.

Hard drive recorders make surveillance more efficient as a result of their high durability and elimination of image degradation caused by repeated recording and ultra fast writing and retrieval. The digital units achieve excellent picture quality with full frame motion-jpeg compression that captures complete images with 720 x 480 pixels – over 500 lines of horizontal resolution – that is clearly superior to conventional time lapse recording technology.

Digital hard drive recorders also offer superior functionality with advanced triplex operation that allows simultaneous live monitoring, recording and reproduction. Layered recording allows individual camera recording and recovery from motion detection, activity detection or hard contact alarm inputs.

In addition, some hard drive units also feature on-board switching capabilities that allow them to be used in a multitude of system applications or as stand-alone mini systems. With an on-board six channel multiplexer, leading units allow up to 16 cameras to be recorded and recovered. Playback and live viewing can be performed on single screen or any of six multi-screen modes. Blocks of cameras can be grouped with up to four cameras per group allowing for individual programming per group. This allows users to save valuable hard drive space by assigning lower recording values to camera groups with lesser priority. Several search methods are available, including the ability to display up to 16 thumbnail displays of each recording sequence. Such advancements have been a significant factor in a new wave of system designs that favor distributed architecture for remote system operation.

Although the advent of digital hard drive recorders represents a new plateau in recording technology for the security industry, numerous applications still exist for conventional tape-based VHS and SVHS format time-lapse recorders, which have been the mainstay recording technologies for security professionals.

Access Control - Biometrics and Iris Recognition

Personal authentication has long been one of the security industry's greatest challenges since traditional forms of identification and access can easily be replicated, lost or stolen. The introduction of easily deployed biometrics systems is alleviating these problems because they are virtually impossible to replicate. This is particularly true of one of the newest biometric technologies, iris recognition, since the technology is non-evasive, virtually impenetrable and does not require a card or proximity device.

Iris recognition authentication has come of age over the last year. Affordable and practically applied systems are now available for both cyber security and access control. Systems are also in development and near market introduction for screening large venues such as the Superbowl and political conventions, which will provide added security with little to no inconvenience for personnel entering a facility, people passing through airports or attending major events.

For cyber security applications, small iris recognition camera systems can be easily networked into a computer system to assure authorized access to sensitive files and programming. Once an individual is in the system, additional layers of security can be implemented to provide secured levels of access for sensitive files and data. The applications for iris recognition cyber security extend beyond conventional network protection to include medical and e-commerce applications, to name a few.

Iris recognition technology is also ideal for access control applications, since it eliminates the use of ID cards, proximity devices and/or passwords that can easily be compromised. When integrated into a security system network, unauthorized attempts to access a facility can automatically notify security personnel and activate programmed video surveillance to provide instantaneous visual coverage and archived video of security breeches.

The same holds true for large-scale systems where groups of individuals or crowds can be authenticated for access, or isolated for additional scrutiny, depending on the system program parameters.

With access control more of a concern than ever before, biometrics, and iris recognition technology in particular, will definitely play an increasing role in homeland defense strategies.

Systems Application - Matrix Switching Technologies

The volumes of information provided by new video surveillance camera technology, digital recorders and access control systems can be overwhelming if not properly managed and controlled. The convergence of digital server and switching system

technologies has culminated in the development of sophisticated matrix switching systems that can handle the large volume of video and data required for sophisticated security system applications on any scale.

Today's advanced matrix switching systems capitalize on the union of digital and analog video technologies on a digital driven platform. Matrix switching systems are available in an array of capacities with large-scale systems capable of handling eight to nine thousand cameras. By designing these large-scale systems in modules, cameras can be added in blocks as facilities expand in physical size, or system parameters extend to include remote facilities – satellite systems – that can be monitored from a central location. By partitioning systems, users can establish full-featured sub-systems while retaining the ability to seamlessly control all satellite systems from a single location. Each satellite system can also be further partitioned with multiple control sites -- providing individual monitoring stations with camera control capabilities over specified camera locations. This can be achieved in a variety of ways using various transmission technologies, including fiber optics and networking, which I will explore in greater detail.

By designing matrix switchers with open architecture, advanced systems can interface with computer-based systems such as access control systems (iris recognition), fire, intrusion and building management systems. In addition, computer driven matrix systems offer security personnel a variety of switching and monitoring operations that enable them to manage large volumes of cameras. For example, cameras can be programmed to switch automatically in "Group", "Tour" or "Group Tour" sequences. "Events" can also be programmed to combine camera-monitor selections with automated camera sequences -- and be automatically triggered by time/date programming or alarm activation. This level of automation takes the burden of system management off of security personnel so they can allocate more time to security services.

Operation of these new matrix switchers can be further enhanced with the addition of powerful graphical user interface software that allows comprehensive system control from a touch-screen computer display. Maps of a facility can be created and displayed on the screen to further facilitate camera control and system features. An integral video frame grabber also allows system operators to view selected cameras directly on the PC display.

The power and capabilities of these large-scale matrix systems are also being incorporated into matrix switchers scaled for smaller installations and remote systems with distributed architecture. These new switching products take advantage of advances in digital and networking technologies that are changing the parameters for video surveillance and security systems where the emphasis has shifted from "closed circuit TV" to networked systems utilizing LAN/WAN technology.

Systems Application - Networking

As previously mentioned, networking has perhaps had the greatest influence over surveillance and security system design over a relatively short time line. Taking a page

from the computer industry, security system networking is performed much in the same manner as a conventional computer network.

Networking interfaces and devices are changing the landscape and architecture for security systems, as we traditionally know it. The advent of networking surveillance systems enables system designers to distribute video surveillance systems equipment – cameras or satellite camera systems – over a much broader system spectrum and geographical area. The effect is that you can easily and efficiently network remote camera locations or many small systems together into a single system – in the same fashion you would tie offices together with a LAN or WAN, such as the Colorado Department of Transportation's traffic control system.

As with any voice and/or data network function, the functionality of such systems is dictated by the network's capacity, or bandwidth. The capacity to process and manipulate video, data and voice signals is determined by the size of the network "pipe". The adaptation of network technology has stimulated the security industry to expand outside of the box and become a "broadband network" industry.

Overall, networking is becoming easier and easier. JPEG compression and HTTP based devices enable the transmission of video and bi-directional control signals using standard web browsers. Simply enter the designated URL address of a camera or satellite system location with a network interface, and you can gain access just like you would your favorite web sites. Connection between multiple network interfaces -- which can be any number of camera locations or satellite systems -- and a LAN can also be established utilizing a series of modems and public lines.

This is a significant development since it provides advanced systems capabilities and video streaming over an Ethernet, and the ability to program, control and monitor video surveillance and security operations using a PC with emulation software or conventional CCTV devices such as a matrix switching system.
Traditional "hard-wired" surveillance and security systems are antiquated by comparison.

The benefits of networking video surveillance and security systems are numerous – from improved cost efficiency to enhanced operations and system capabilities. Security professionals also can use network technology to verify alarms by comparing video feeds of facilities with images stored in memory. This capability provides highly efficient off-site central monitoring with the ability to quickly and cost-effectively respond to alarm conditions -- and provide the added safety feature of determining the status and threat potential of intruders.

The most pervasive means to achieving network accessibility is the Internet – which offers a fast and practical means to access a LAN or modem based WAN video surveillance or security system interface. Internet access offers significant cost efficiencies by enabling network video surveillance and security system monitoring and control from virtually any location in the world. The proliferation of transmission modes

such as digital cellular service and portable satellite devices extends the applications for remote access even further.

On a more practical level, the utilization of standard telephone lines for network and/or Internet connection provides security professionals with a tremendous opportunity for system expansion and industry growth. Network/Internet connection also permits a new level of off-site control capabilities -- on a global scale -- for centralized intra-facility security operations.

New installations would benefit most by exploring the networking options available today as a means to easily upgrade or expand the scope of operations.

Convenience Issues:
When you combine all of the aforementioned surveillance and security technologies, the resulting system capabilities are quite impressive by any standard of measure. Today's video surveillance and security technologies bridge analog and digital platforms to offer new levels of system control, performance and coverage. The ability of security personnel to monitor large or remote systems from a central location, while allowing field personnel to autonomously control their satellite systems, unifies and fortifies what were previously independent operations by separate field offices.

The use of artificial intelligence in the form of programmable video surveillance events and facility "tours" automates security operations and intensifies personnel focus and coverage capabilities. These capabilities are best exemplified through the application of matrix switching technologies supported with sophisticated control software.

With any video surveillance activity, there are privacy issues to address. However, in lieu of recent events, safety and security also have become high priorities. By establishing clear security objectives for both security staff and personnel, and forming a relationship between the two that advocates service and safety, high security environments can co-exist with continued regard for personal freedoms.

Obstacles to Greater Government Agency Use of Security Technology:
Security operations have been thrust into the limelight unlike any other time in our nation's history. Federal buildings that once were protected by a handful of guards, antiquated CCTV cameras and metal detectors are now being barricaded with concrete facades, night vision technologies and chemical detectors. Our perceptions of a safe and secure environment have dramatically changed.

Budget and education are the two most common factors that constrain security operations by government agencies. Security operations typically suffer during economic downturns, as agencies reduce budgets in favor of personnel and away from equipment spending. Additionally, security professionals in Federal agencies continue to struggle with keeping pace with today's rapid development of new video surveillance and security technologies.

In light of our nation's tightened security concerns, budget issues concerning security now are being readdressed across the country in both public and private sectors. Manufacturers of video surveillance and security systems equipment, however, need to provide more education opportunities to the government to keep them apprised of new technology developments. This will foster the intelligent deployment of new systems technology where it is most needed, as budgets become available.

Another problem that has hampered the modernization of security in Federal buildings is the lack of set standards. Although "specs" are frequently issued for new installations and system updates, they are too general. This allows bidding dealers too much leeway in specifying equipment, which leads to incompatibility problems within facilities – making network connection between facilities virtually impossible.

Recommendations:
Government agencies and departments responsible for security need to establish stronger partnerships with manufacturers and distributors of security products. As mentioned, the industry can provide education on the latest developments in technology and supplement the relationships that exist between systems integrators and government security personnel. For instance, Panasonic already has a national education program available at no charge to the government. The industry also is developing new educational programs that can be made available to government security personnel during security conferences and trade shows.

One of the priorities for securing Federal buildings should be the establishment of a set standard that outlines the measures to be taken in the three identified zones of protection. This will help assure minimal levels of security at every facility and bring attention to present deficits. The standards also should include more thorough specifications to assure greater levels of performance, compatibility and future system expansion.

Summary:
The most advanced technology is now available to fortify our Federal buildings and campuses and to integrate it with current systems. In addition, the security industry offers the services of trained professionals who have the technological and security operations expertise to secure our government's infrastructure and to secure our homeland.

Thank you again for this opportunity to share with you my perspectives on the extent of security technologies now available to protect our Federal government buildings. I look forward to answering any questions you may have regarding the newest security technologies and my comments on ways the government may better secure its buildings.

Mr. TOM DAVIS OF VIRGINIA. Thank you. Mr. Bordes, if we can try to get you in, if you can do it in about 4 minutes, we can get all the testimony out of the way and come back for questions.

Mr. BORDES. I'll try, sir. Good afternoon, Mr. Chairman, members of the subcommittee and distinguished guests. I would like to take this opportunity to thank you for allowing me to present this information on behalf of the private security industry and as a member of the American Society for Industrial Security.

As a professional security consultant working in the private sector, I have over 25 years experience in the disciplines of threat analysis and countermeasures design. ASIS, with more than 32,000 members, is a preeminent international organization for security professionals. We have chapters in almost every country in the free world.

There are three subjects I would like to address in today's presentation. The first will be how the private sector evaluates threat vulnerabilities and ultimately selects countermeasures to protect assets.

Second, I will cover how that group works to develop the balance of security measures with convenience and protection of privacy for employees and visitors.

Finally, I would like to present some of the new philosophies of security that have developed within the corporate world since September 11th.

The private sector has for many years accepted the fact that a high percentage of security-related incidents of either general criminal activity or specific target action, such as workplace violence, can be attributed to the unauthorized individual gaining access to a facility. The approach to threat and vulnerability analysis has been to identify the layers of protection required to either deter or detect and neutralize a perpetrator prior to achievement of their objective.

To accomplish this, basic technologies such as card access, biometrics, closed circuit surveillance and intrusion detection are combined into an integrated electronic security system. In determining how to protect the facilities, security assessment will address subjects such as local environment, facility use, total value of the asset, the possibility of a threat being successfully carried out, and the criticality level related to either partial or total loss of that asset.

This approach can be applied to any scenario that ranges from protecting the CEO to ensuring that nuclear weapons are properly secured. The implementation of security measures does not, however, have to inflict the penalty of inconvenience or loss of privacy upon those working within the protected environment.

The designed effort must ensure protection while at the same time maintaining the focus of developing user-friendly and non-intrusive security measures. Well-designed security programs should ultimately result in minimal contact with the subject and with all verification and surveillance being totally transparent to anyone other than the security team.

As you all know, the invasion of privacy debate over the use of closed circuit television systems has gone on for years. This same argument will move to a higher plane as biometric template data

bases become a reality. However, in the private sector, the trend has been for several years to develop surveillance teams that are reactive as opposed to passive, and to focus on using these same systems for security incident assessment as opposed to general surveillance.

Even the American Civil Liberties Union has acknowledged the fact that people are more open to the use of surveillance systems based on the acceptance of the need for more security. Hence, the private sector has worked diligently with manufacturers and software development entities to ensure that data base access and abuse incidents are reduced to the lowest number possible by protecting access to sensitive information.

Advances in the technologies of digital recording, as well as the ability to transmit signals over LAN, WAN, or GAN, has had a major impact on the effectiveness of security assessment. Today the security console officer of a global corporation can, through the use of proprietary network transmissions, receive real-time video, intrusion alarm data and access control transaction information from any company within the facilities around the world.

Technologies currently being developed will further enhance security protection techniques by being able to lock onto a subject or an object for the purposes of tracking with a camera system. Should the subject go from one camera viewing area to another, the tracking process will roll over to the other camera in order to maintain surveillance.

The use of biometric technology, such as finger and hand geometry, facial recognition, iris scan, retinal scan and other methods of providing positive identification, will have a definite impact on the design of access-controlled systems.

A recent poll of systems integrators indicated that 66 percent of their clients either had installed biometric systems or were considering implementing the technology within the near future.

September 11th has created an attitude of acceptance on the part of many Americans for increased security measures. One of the most significant within the private sector is the acceptance of the need to positively identify persons entering controlled areas. This decision has impacted the use of biometric verification techniques in private and government security programs. In fact, in the private sector, security has been a top priority, with money set aside for upgrades and new installations.

Additionally, facilities such as water treatment plants, power generation stations are now implementing security measures that incorporate the whole gamut of electronic protection devices.

Therefore, in summary, I would submit that in the private sector, one will no longer hear the phrase that's never happened here. We have been awakened to the fact that attacks can be carried out against our Nation and our workplaces and any place we gather in large numbers, such as the current threat from the FBI about malls. With the increased threat related to the use of biological/chemical agents, suicide bombers and weapons of mass destruction, the development of security measures in both the private as well

as the Government sectors will continuously be improved upon and implemented to protect the people of this great Nation. Thank you again for allowing me time for this presentation and God bless America. I will now entertain questions.

[The prepared statement of Mr. Bordes follows:]

Testimony Of

ROY N. BORDES
President/CEO
The Bordes Group Inc.
Orlando, Florida
And
Council Vice President
American Society for Industrial Security (ASIS)

As Presented to

UNITED STATES CONGRESS
HOUSE OF REPRESENTATIVES
SUBCOMMITTEE
ON
TECHNOLOGY AND PROCUREMENT POLICY

Representative Thomas Davis III, (R-VA) Chairperson

April 25,2002
2 PM
Room 2154
Rayburn House Office Building

Good afternoon, Mr. Chairman, members of this Subcommittee on Technology and Procurement Policy, and distinguished guests. I would like to take this opportunity to thank you for allowing me to present this information on behalf of the private security industry and as a member of the American Society for Industrial Security (ASIS). As a professional security consultant working in the private sector, I have over 25 years experience in the disciplines of threat analysis and countermeasures design. ASIS, with more than 32,000 members, is the preeminent international organization for security professionals. We have chapters in almost every country in the free world.

There are three subjects I would like to address in today's presentation. The first will be how the private sector evaluates threats-vulnerabilities and ultimately selects countermeasures to protect assets. Secondly I will cover how that group works to develop the balance of security measures with convenience and protection of privacy for employees and visitors. Finally, I would like to present some of the new philosophies of security that have developed within the corporate world since September 11th.

The private sector has, for many years, accepted the fact that a high percentage of security related incidents, of either general criminal activity or specific target actions such as workplace violence, can be attributed to the unauthorized individual gaining access to a facility. The approach to threat and vulnerability assessment has been to identify the layers of protection required to either deter or detect and neutralize the perpetrator prior to achievement of their objective. To accomplish this, basic technologies such as card access, biometrics, closed circuit surveillance, and intrusion detection are combined into an integrated electronic security system. In determining how to protect a facility, security assessments will address subjects such as local

environment, facility usage, total value of the asset, the possibility and probability of a threat being successfully carried out, and the criticality level related to either partial or total loss of that asset. This approach can be applied to any scenario that ranges from protecting the CEO to ensuring that nuclear weapons are properly secured.

The implementation of security measures does not however have to inflict the penalty of inconvenience or loss of privacy upon those working within the protected environment. The design effort must ensure protection while at the same time maintaining the focus of developing user friendly and non-intrusive security measures. Well designed security programs should ultimately result in minimal contact with the subject and with all verification and surveillance being totally transparent to anyone other than the security team.

As you all know, the invasion of privacy debate over the use of closed circuit television systems has gone on for years. This same argument will move to a higher level as biometric template databases become a reality. However, in the private sector, the trend has been for several years to develop surveillance systems that are reactive as opposed to passive[i] and to focus on using these same systems for security incident assessment as opposed to general surveillance. Even the American Civil Liberties Union has acknowledged the fact that "people are more open to the use of surveillance systems[ii]" because of the acceptance of the need for more security. Hence the private sector has worked diligently with manufacturers and software development entities to ensure that database access and abuse incidents are reduced to the lowest number possible by protecting access to sensitive information.

Advances in the technologies of digital recording as well as the ability to transmit video signals over the LAN, WAN, or GAN[iii] has had a major impact on the effectiveness of security assessment. Today, the security console officer of a global corporation can, through the use of proprietary Network transmissions, receive real time video, intrusion alarm data, and access control transaction information from any of the company's facilities around the world.

Technologies currently being developed will further enhance security protection techniques by being able to lock onto a subject or an object for the purposes of tracking with a camera system. Should the subject go from one camera's viewing area to another, the tracking process will roll over to the other camera in order to maintain surveillance.

The use of biometric technologies such as finger and hand geometry systems, facial recognition, Iriscan, retinal scan, and other methods of providing positive identification will have a definite impact on the design of access control systems. A recent poll of system integrators indicated that 66% of their clients either had installed biometric systems or were considering implementing the technology within the near future.[iv]

9/11 has created an attitude of acceptance on the part of many Americans for increased security measures. One of the most significant within the private sector is the acceptance of the need to positively identify persons entering controlled areas. This decision has impacted the use of biometric verification techniques in private and government security programs. In fact, in the private sector, security has become a top priority with monies being set aside for upgrades and new installations. Additionally, facilities such as water treatment plants and power generation stations are now

implementing security measures that incorporate the whole gamut of electronic protection devices.

Therefore in summary I would submit that in the private sector, one will no longer hear the phrase, "that's never happened here." We have been awakened to the fact that attacks can be carried out against our nation, in our workplaces, and any place we gather in large numbers. With the increased threats related to the use of biological/chemical agents, suicide bombers, or weapons of mass destruction (WMD), the development of security measures in both the private as well as government sectors will continuously be improved upon and implemented to protect the people of this great nation.

Thank you again for allotting time for this presentation and **God Bless America**! I will now entertain questions from the members of the committee.

---

[i] Reactive camera systems are designed to activate when an event takes place as opposed to passive systems which depend upon the event being detected by the human watching a monitor.
[ii] Interview with Mr. Jay Stanley, Privacy public education coordinator for the American Civil Liberties Union (ACLU), Security Sales – January 2002, page 44
[iii] LAN – Local Area Network, WAN – Wide Area Network, GAN – Global Area Network
[iv] Security Scanner survey – Security Sales – April 2002 page 16

Mr. TOM DAVIS OF VIRGINIA. Thank you very much. There is a series of three votes. We're going to be at the end of one vote, so hopefully it will move quickly. But I'll declare a recess. It will probably be 20 minutes or so. Feel free to move about and be back here in 20 minutes.

[Recess.]

Mr. TOM DAVIS OF VIRGINIA. We're ready to start the questioning. I'm going to start with Mrs. Davis, the gentlelady from Virginia.

Mrs. JO ANN DAVIS OF VIRGINIA. Thank you, Mr. Chairman. And thank you, gentlemen, for being here. I apologize I couldn't be here to hear your testimony. I had several markups at the same time.

My first question is for Mr. Moravec. As the Government's biggest landlord, how do you work with building tenants to determine the security needs and the products required?

Mr. MORAVEC. I'm sorry, Congresswoman, I didn't hear the question.

Mrs. JO ANN DAVIS OF VIRGINIA. As the Government's biggest landlord, how do you work with the building tenants to determine the security need and products required?

Mr. MORAVEC. Fundamental to our security philosophy is the understanding that each building constitutes a very distinct set of security and safety needs. So it has been our philosophy to work with the building security committee of that building. Every Federal building has a building security committee, sometimes called an occupant emergency organization, that is responsible for developing, in consultation with the Federal Protective Service, plans for the safety and security of the occupants and visitors to that building. So it's very individualized.

Mrs. JO ANN DAVIS OF VIRGINIA [presiding]. If you'll pardon me for changing seats there real quick. As a followup, what purchasing assistance does GSA provide to Government agencies interested in acquiring security technologies?

Mr. MORAVEC. I'll defer to Wendell Shingler.

Mr. SHINGLER. Actually we do a wide variety of things. We provide consulting services for the most part of going into a Federal agency and making recommendations on how to offset their vulnerabilities. On the flip side of that, the Federal Supply Service within GSA and our folks work in consultation to come up with contracts that would meet the needs to provide those items, cameras, monitors and the like for not only us but the individual departments and agencies.

Mr. MORAVEC. Federal Protective Service is assessing its own needs all the time for the buildings that are GSA-controlled. We also, through interagency groups, for example, the Interagency Security Committee share information with security personnel at other agencies and departments of Government as to technologies that are emerging, technologies that have been proven to be especially effective. We definitely talk amongst ourselves within the Federal community.

Mrs. JO ANN DAVIS OF VIRGINIA. Do you feel you can do it in a timely manner since apparently it's going through several different agencies?

Mr. MORAVEC. Well, it's an ongoing process. We are in constant dialog with each other. Within the Federal Protective Service we have been assessing new technologies on a somewhat ad hoc basis. We're now taking steps to create a standing committee within our organization of specialists who will be proactively involved in seeking out new security technologies. And clearly, since September 11th we're now aware of and defending against a much broader range of threats to Federal facilities. So it's very important that we be preemptive and proactive.

Mrs. JO ANN DAVIS OF VIRGINIA. Mr. Bordes, what has been the impact on demand since the September 11th terrorist attacks, and can the industry adequately meet the increased demand in a timely basis? And if not, who is stepping in to fill that role?

Mr. BORDES. I was working the mic. I didn't hear the last half of your question.

Mrs. JO ANN DAVIS OF VIRGINIA. If you're not able to do it in a timely basis, who is stepping in to fill that role if the industry can't do it?

Mr. BORDES. Well, the private sector is doing a lot of things to try to meet the threats that they now perceive after September 11th. The industry security has in some areas been able to meet that need. However, there are other technologies that the private sector is calling upon that probably a year ago the delivery date on that technology was 3 to 4 weeks, now that delivery date is 5 to 6 months. And it depends on the technology that you're addressing.

But the private sector is really working very diligently to try to upgrade the security across their operation, as the Government is, and it's just an issue of supply and demand. The industry really is in some segments very, very small.

In fact, the area of biometrics up until a couple years ago, each biometric was basically manufactured by one company. So these companies were not really geared up for to you walk in and say I need 1700 hand geometry readers. It would really blow them back.

Mrs. JO ANN DAVIS OF VIRGINIA. You said that before September 11th it would have been 3 to 4 weeks but now it's 5 to 6 months. That's because there is so much more demand?

Mr. BORDES. Because of supply and demand.

Mrs. JO ANN DAVIS OF VIRGINIA. Who would step in or is there anyone to step in, in that interim?

Mr. BORDES. In some technologies, ma'am, there is nobody to step in.

Mrs. JO ANN DAVIS OF VIRGINIA. In some. But how about others?

Mr. BORDES. In others that are companies that are gearing up, companies that are in closed circuit television system, like Panasonic and these people, they are able to immediately increase output and to meet the needs. But in some sectors, like hydraulic bollards, vehicle barriers, motorized gates, crash gates for embassies, airports, this type situation, they're just not geared up to manufacture them that quickly.

Mrs. JO ANN DAVIS OF VIRGINIA. My time is up, but I thank you, gentlemen.

Mr. TURNER. Thank you. I unfortunately missed your testimony. I was on the floor debating an amendment to the INS reform bill.

I was just curious, in looking through some of the testimony, is there a general agreement as to which technologies should be employed, or are we still at the point where there are so many different ones out there that nobody is really settled in on which ones are best? And I'd welcome any of your comments on this.

Mr. MORAVEC. I'll take a stab at that. I think there's general agreement in the Federal community as to what the appropriate technologies are and how they ought to be generally deployed. As I testified earlier, Congressman Turner, we look at each building as a separate and distinct security threat and try to craft a package of countermeasures that address the vulnerabilities that we have assessed at a particular building. And it's a package of things that includes deployment of manpower, contract guard services, specific electronic countermeasures like magnetometers, x-ray machines, explosion detection devices. So it's a combination of both technology and manpower deployment and operations that really constitute a well-rounded security program. And I think there is general agreement in the Federal Government. The packages vary, depending on the perceived threat. Buildings can be perceived as having a higher or lower threat. So there's quite a bit of diversity or at least a range in terms of the intensity, if you will, of the security deployment at a particular building, depending on what the perceived level of threat is.

Mr. TURNER. I guess I was particularly interested in the biometrics area because it seems to me that, No. 1, the Federal Government should take the lead in trying to establish some standard there because once the Federal Government moves forward with the application of a given technology, it seems that it probably encourages the private sector and smaller purchasers to choose the same. And over time it would seem to me important to the Nation to have some standardization. If we all are walking around with cards that swipe and we could get in several places with that card or if we're going to rely on retinal scan technology, then others would adopt that and we become more standardized and access would be more readily afforded to the public in general if there was some standardization. Am I correct in that?

Mr. MORAVEC. I completely agree with you. This is an opportunity for the Federal Government to show leadership to the private sector. The grim reality is that since Oklahoma City, the Federal Government, including the Federal Protective Service, have become very knowledgeable about ways of designing and building and defending buildings against different kinds of threats. And even we are very actively reaching out to the private sector through groups like the American Security Society for Industrial Security and through different real estate organizations to try to share that information with them.

However, the Federal Government at this point in time, itself not being a monolithic entity, has a variety of different responses with regard to identity cards. With 100 different agencies, 100 different agencies have 100 different kinds of identity cards. That is part of the challenge of defending buildings. For us to show leadership with regard to access cards, whether they include biometric cards or not, or whether they're smart or not, the Federal Government

needs to get together and decide on, I think, on a national government card.

Mr. TURNER. What would it take to accomplish that? Obviously we now have all these agencies, as you say, going out there adopting whatever system they want to put in place. What would it take to have some standardization accepted in our Federal agencies?

Mr. MORAVEC. Well, I think that direction could certainly come from the executive branch. It could come through GSA. It could come through the Office of Personnel Management. It could come through the offices of the Homeland Security. There are a number of different places where that direction could come from.

Mr. TURNER. Thank you. Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA [presiding]. Thank you very much. Mr. Abram, let me ask you a question. Because of the heightened and immediate need for advanced security products and system components for our government facilities, are there any current constraints with the U.S. Government being able to quickly source the kind of equipment needed for security?

Mr. ABRAM. I believe there are. And I believe the potential exists for even greater problems. The Buy America laws require the U.S. Government to source from domestic suppliers and, if not available, from suppliers in countries that have signed onto an international procurement agreement. In Asia, that includes only Hong Kong, Japan, Korea, and Singapore. Now because of globalization and economies of scale concerns, many of the security manufacturers, Panasonic included, are finding that they are moving to countries that can manufacture less expensive for us, countries like China and the Philippines. And this is a possible restraint in the Government purchasing product from organizations such as Panasonic.

Recognizing this constraint at a time of increased security demands, the SARA, the Services Acquisition Reform Act of 2002 that Chairman Davis introduced, provides an exemption for this sourcing restriction for information technology commercial items. Because of the importance of the homeland security, the proposed legislation defines information technology to include imaging peripherals and certain devices necessary for security and surveillance. It is through the SARA that we will be able to correct some of these problems that are going to become more and more evident, at least in the video surveillance area.

Mr. TOM DAVIS OF VIRGINIA. Let me ask Mr. Rhodes. The biometric technologies that were identified within your presentation represented several different technologies. Which technologies are actually in use and which do you believe are the most effective for security identification verification purposes? Or do you think it depends?

Mr. RHODES. Out of all of the biometric technologies, there is really only one that we couldn't find in pervasive use and that was signature recognition. The most prevalent technology biometric technology is the fingerprint scan, and that's because it grew out of law enforcement and it's the most established technology, the most established procedure for enrolling an individual into the system, and that's reflected in its price as well. It's only about $4 per user if you already have the server in place.

From our analysis, the biometric technology that probably shows the most promise is the iris scan. That technology is going to advance because it's the least invasive to the individual. As was stated in an earlier statement from Panasonic, as the quality of the camera for both movement and room light improves, you can stand farther and farther away from the receptor, so people don't get the feeling of having it invade their body. And that's probably going to always be a resistance to somebody like a retina scan where you have to sit still for quite a long time while it scans the back of your eye. And so in a nutshell, the fingerprint scan is the most pervasive and the scan for iris is the one that probably has the best future.

Mr. TOM DAVIS OF VIRGINIA. Fingerprint scan is fast. Isn't it pretty efficient?

Mr. RHODES. Yes. In some cases you can get it down to just a couple of seconds. As a matter of fact, it's being used currently by the FAA in some of their facilities for quick access to some of the doors, some of the secured access facilities.

Mr. TOM DAVIS OF VIRGINIA. Let me ask Mr. Moravec and Mr. Jester about the use of biometric technologies. Are we using that widely in Government and are we restricting the use of the personal information that's stored?

Mr. MORAVEC. In the Federal Protective Service we are not at this point, to my knowledge, deploying what could accurately be called biometric technology with regard to access cards or access controls.

Mr. TOM DAVIS OF VIRGINIA. How hard and difficult would it be to do that?

Mr. MORAVEC. It would be difficult for me to assess, sitting here, how difficult it would be. It would clearly be—given the scope of our portfolio, which encompasses over 8,000 buildings and 340 million square feet, applying anything consistently and effectively on a base that big would certainly be logistically challenging.

Mr. TOM DAVIS OF VIRGINIA. Right. OK.

Mr. JESTER. We're using biometrics at specific locations where you have a very sensitive office within a building. We're using iris scan, we are using hand geometry readers. There are limits of where we do use it. We don't use it in the entrance to the facility because at the Pentagon, for example, we have 20,000 employees and everybody going through it would be a long line waiting to come in. But we do use it at specific locations.

The U.S. Army is leading an effort within the Department of Defense to look at—they have a biometric officer. They're looking at different applications of the biometric technology and looking where it can be used within the Department of Defense. So there is a program to encourage the use of biometrics.

Mr. TOM DAVIS OF VIRGINIA. OK. Mr. Moravec, let me ask you. The Federal Protective Services are responsible for protecting Federal buildings. Do they use the same approach to designing countermeasures as would be found in the private sector?

Mr. MORAVEC. Yes. Yes. In fact, we have a very close working relationship with the American Society for Industrial Security, absolutely.

Mr. TOM DAVIS OF VIRGINIA. Mr. Bordes, what services can you offer to Federal security planners who are working to better protect Federal facilities? What recommendations does GSA give to these planners?

Mr. BORDES. I think one of the most important things on Federal protection, developing Federal protection of facilities, is to get involved in the planning process early. That's one of the major problems that we see as, you know, from reading my information, I run the GSA FPS training program for physical security. And that particular program, we really try to stress to our people to get involved early in the planning to make sure that they have the input to be able to address situations such as barriers, setback, glazing of glass, or hardening of facility and this type of situation.

The people in FPS basically use the same measures that the private sector does. They go out, they identify the threat, they try to find countermeasures that will address that threat, and then they address the issues of how they're going to respond appropriately and also run the educational program. But one of the major problems seems to be basically the issues of planning. It's important that in any design, in any security design, whether it's private sector or whether it's Government or whether it's military, that the people who are doing the design get involved in the process early on. Because there are a lot of things that go into a design that if you come in at a late stage in the design are extremely difficult and extremely expensive to implement. That seems to be a problem that is always being confronted by people who are designing the GSA security programs.

Mr. MORAVEC. If I could respond to that. Since Oklahoma City, we have obviously been designing and building buildings in a completely different way. We have stringent setback criteria. We employ anti-progressive collapse technology in their design. We have hardened curtained walls, ballistic glass. Up until September 11th, we were primarily defending against what happened at Oklahoma City, which was the breaching of perimeter security by a truck bomb and the total collapse of the building. I think what Mr. Bordes is saying is absolutely correct. It's very important that Federal Protective Service trained physical security people and consultants, as well as building managers, be involved with architects and engineers in the design of buildings. We make every effort to make sure they have a seat at the table and, of course, even more so than since September 11th.

Mr. TOM DAVIS OF VIRGINIA. There is always a tendency for generals to fight the last war. So you defend against Oklahoma City and now we look back to September 11th, defend against that. I mean, we are being proactive in figuring out what else could go wrong.

Mr. MORAVEC. We are. Especially since the anthrax episodes, we're looking at the location of air intakes, we are looking into the purchase and deployment of equipment that can detect toxins in the building's water or air supply and devices to automatically take corrective action in that event. September 11th has really opened a whole new vista to us in terms of ways that people can—who wish us ill can do harm to people and to buildings.

Mr. TOM DAVIS OF VIRGINIA. Yes. Let me ask both Mr. Jester and Mr. Moravec, how do you determine the proper balance between security and convenience and efficiency? To some extent, if you want to make a building entirely secure, it's going to be a real pain for somebody trying to get in and out some of the time. You can make it secure, but you also have to make it functional. It's a difficult balance, remembering most of these buildings will probably never undergo any kind of problem. How do you get that balance?

Mr. JESTER. I think it begins—the word planning has been used. Having gone through—having been about 300 feet from where the plane hit, a lot of lessons were learned. The key word is planning. And planning goes in this particular application, too. If we're looking for a location for a, for example, a DOD operation, we need to be careful on where we place that. We can't select the wrong building. If we put a very sensitive DOD operation—and we're not just concerned for terrorism, we're also concerned for foreign intelligence-gathering. So it has to be some care exercised simply—it's not simply a selection of how many square feet that building happens to be, we should not be putting a building or an operation into a building where there's a lot of highly public agencies in that building, for example, Social Security. We should not be mixing those organizations together. But it is a delicate balance. So we say it begins right in the very beginning, put them in the right location.

If you, for example, take agencies with high security requirements and lump those together in those kinds of buildings where it can be more secure, don't mix and match high secure requirements with organizations that have a high public contact.

Mr. TOM DAVIS OF VIRGINIA. OK.

Mr. MORAVEC. That's certainly beneficial. Just for the General Services Administration, we are determined not to build bunkers. We are determined to build buildings, iconic buildings, 100-year buildings that are emblematic of the spirit of the American people, that are first and foremost secure, but are also esthetically pleasing and hopefully an adornment to the communities where they're located.

We are very cognizant of avoiding—creating a climate of fear at buildings which is often present when you take especially stringent security measures. We want, as someone put it, I thought very well, we want to first welcome and then challenge people who are coming to the building, to do both, but to do it in a way that is not oppressive and is not obtrusive. And this is particularly challenging in courthouses. We're building a lot of courthouses across the country now, and we want those buildings to be like the American judicial system itself, open and accessible to all. But obviously at a courthouse in this day and age, those buildings need to be very secure.

So it is a continuing challenge and one that we spend an awful lot of time thinking about and working on.

Mr. TOM DAVIS OF VIRGINIA. Yes. I worked here in the 1960's as a page and you could drive in here at night, anybody could come in here at night. You didn't have the metal detectors and everything to get in and out of the building. It worked pretty smoothly.

But I guess the world changes and you have to change with it. Somehow I would like the world to change back. It would be a lot more efficient in terms of how we could spend or money.

In the meantime, you all have a very difficult job. Every time something goes wrong, everybody is going to second-guess you. To the extent that you are spending money doing these kinds of things, you can't do other things.

Mr. MORAVEC. Well, as has been brought out by several of the witnesses, it really is a package of different countermeasures that really need to be undertaken. I mean we are expanding our guard contracts, we've enhanced the training and testing of our different kinds of countermeasures. We have very close involvement these days with the FBI and the CIA and different joint terrorism task forces. We are engaging security measures in major metropolitan areas to try to design security countermeasures in areas that are particularly densely populated with Federal workers that are not obtrusive. We are spending a lot of time in the buildings talking to the tenants and to the different building security committees about what they can do specifically to protect themselves. We're really trying to help the Federal associates and people who are visitors to Federal buildings move themselves to a higher state of vigilance and wariness which is, I think, necessary in this day and age.

Mr. JESTER. There was a failure, I think, on September 11th. It was probably, I would say, a failure of imagination. We have to in that particular field, we have to use our imagination and not, as you said a while ago, fight the last war. We have to look forward and think about what could happen.

Years ago I think everybody in this country was shocked when someone went into a McDonalds in California and killed 21 people. We were shocked by that. We were shocked later on when school kids were shooting each other in school.

So in our profession we need to be looking forward and almost to some degree have screen writers look about what things could happen. I don't think anyone would imagine the Pentagon—we had talked about planes hitting the building because we are very close to the airport, as an accident or maybe as a small aircraft. But never did we dream of a 757 coming into our building.

So we need to use our imagination to think about what kinds of things could happen and then go back to that key element of having some plans and not think it won't happen on our watch. If we think it's not going to happen on our watch, we don't plan for it. So we need to do proper planning and then use all the technologies that are available to us. The technologies are great, they're fantastic tools, but to use those technologies as tools and be careful how we use them because we—as you learned, one of the biggest technologies that failed us on September 11th was the cell phones. We could not communicate throughout the entire city on cell phones. So using technologies, we ought to also go back to some very basic principles of planning and exercises and drills.

Mr. TOM DAVIS OF VIRGINIA. Thank you.

Mrs. Davis.

Mrs. JO ANN DAVIS OF VIRGINIA. Thank you, Mr. Chairman. These questions are probably just curious questions. But I think,

Mr. Rhodes, you talked about the fingerprinting scan and the iris scan.

Mr. RHODES. Yes, ma'am.

Mrs. JO ANN DAVIS OF VIRGINIA. And Mr. Abram said that some of the technology was not available through Buy America. Would any of those be available through Buy America?

Mr. RHODES. I don't know the underlying—I think that at least some of the vendors on the GSA list would be available. I don't know that they would be available in the quantities that people would need. The fingerprints is very well established, so you'd probably be able to gear up for the procurement. But on the retina scan, that's still developing technology. So I don't know that would be—you would be able to buy it on the scale that you would need.

Mrs. JO ANN DAVIS OF VIRGINIA. On the iris scan—and somebody said they were using that now, I think you did, Mr. Jester. That's the colored part of your eye, right? That's the colored part of your eye, right?

Mr. JESTER. Yes, ma'am.

Mrs. JO ANN DAVIS OF VIRGINIA. If someone has one of those colored contact lenses, how does that affect it?

Mr. ABRAM. I believe I can answer that. It really does not unless they are extremely dark, dark colored lenses, and then it would give you a negative access through the access control. The product takes—basically takes a picture of the iris, digitizes that picture into a 512 bit picture or 512 bit data image that is then used for comparison purposes. So as long as it is a coloring or tint in the contact lenses and a coloring or tint in your glasses, there is no effect or adverse effect from reading it. As you get much darker tints to both of those glasses and contacts, it will have an effect.

Mrs. JO ANN DAVIS OF VIRGINIA. Mr. Jester, the planes that hit the Pentagon and the Twin Towers, I'm not sure there's any security measures that we could have taken in either of those buildings for that.

Mr. JESTER. No, ma'am. I was asked by the press do we have guns on the roof. That will start with the airport security. It has to be at that point. Because we can't stop it in our building. We can be better prepared for that. And I think one of the things that we feel successful about was in the preceding year we had been doing drills with the employees, evacuation drills outside the building, as well as sheltering-in-place drills. So—because most employees in Federal buildings got their last instruction on fire drills when they were in the third grade. So we pushed that for a year. And so when we activated the alarms that day, I think we had less problems because people had actually been prepared by having drills.

Mrs. JO ANN DAVIS OF VIRGINIA. Thank you, gentlemen. Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you all. Before we close, I want to take a moment to thank everyone for attending today's subcommittee hearing. Thanks for bearing with us as we went over and voted and came back. Our special thanks to the witnesses, to Representative Turner, Mrs. Davis, and other attendees. I also want to thank my staff for organizing what I consider to be a very productive hearing. I'm going to enter into the record the briefing

memo that was distributed to subcommittee members. We'll hold the record open for 2 weeks from this date for those that want to forward submissions for inclusion into the record.

These proceedings are closed.

[Whereupon, at 3:45 p.m., the subcommittee was adjourned.]

○