United States Government Accountability Office

GAO

Report to the Chairman, Committee on Government Reform, House of Representatives

November 2004

HOMELAND SECURITY

Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices

GAO-05-49

November 2004

HOMELAND SECURITY

Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-49, a report to the Chairman, Committee on Government Reform, House of Representatives

Why GAO Did This Study

The war on terrorism has made physical security for federal facilities a governmentwide concern. The Interagency Security Committee (ISC), which is chaired by the Department of Homeland Security (DHS), is tasked with coordinating federal agencies' facility protection efforts, developing protection standards, and overseeing implementation. GAO's objectives were to (1) assess ISC's progress in fulfilling its responsibilities and (2) identify key practices in protecting federal facilities and any related implementation obstacles.

What GAO Recommends

GAO is recommending that DHS direct ISC to develop an action plan that identifies resource needs, goals, and time frames for meeting its responsibilities; and proposes strategies for addressing the challenges it faces. Furthermore, GAO recommends that the Chair of ISC, with input from ISC member agencies and considering GAO's work as a starting point, establish a set of key practices that could guide agencies' efforts in the facility protection area. This initiative could be used to evaluate agency actions, identify lessons learned, and develop strategies for overcoming challenges. DHS concurred with the recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-49.

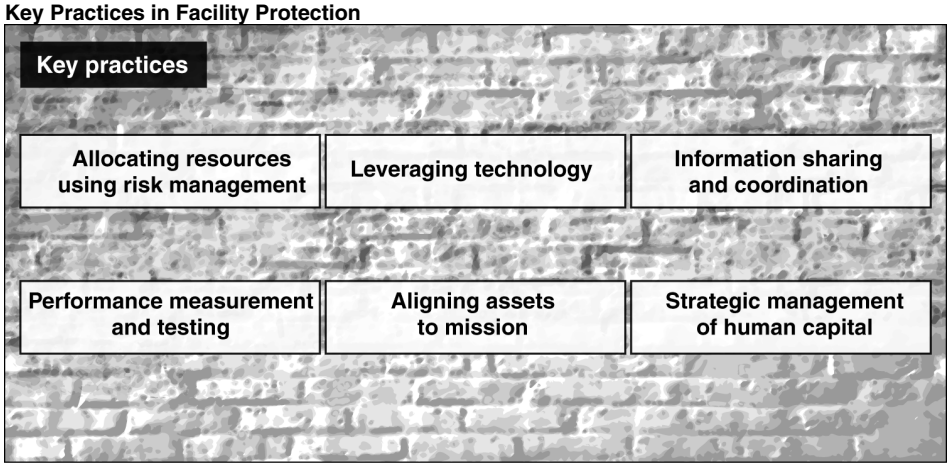
To view the full product, including the scope and methodology, click on the link above. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

What GAO Found

ISC has made progress in coordinating the government's facility protection efforts. In recent years, ISC has taken several actions to develop policies and guidance for facility protection and to share related information. Although its actions to ensure compliance with security standards and oversee implementation have been limited, in July 2004, ISC became responsible for reviewing federal agencies' physical security plans for the administration. ISC, however, lacks an action plan that could be used to provide DHS and other stakeholders with information on, and a rationale for, its resource needs; garner and maintain the support of ISC member agencies, DHS management, Office of Management and Budget, and Congress; identify implementation goals and measures for gauging progress; and propose strategies for addressing various challenges it faces, such as resource constraints. Without an action plan, ISC's strategy and time line for implementing its responsibilities remain unclear.

As ISC and agencies have paid greater attention to facility protection in recent years, several key practices have emerged that, collectively, could provide a framework for guiding agencies' efforts. These include allocating resources using risk management; leveraging security technology; coordinating protection efforts and sharing information; measuring program performance and testing security initiatives; realigning real property assets to mission, thereby reducing vulnerabilities; and, implementing strategic human capital management, to ensure that agencies are well equipped to recruit and retain high-performing security professionals. GAO also noted several obstacles to implementation, such as developing quality data for risk management and performance measurement, and ensuring that technology will perform as expected.

Key Practices in Facility Protection



Source: GAO.

Contents

Abbreviations

CARES	Capital Asset Realignment for Enhanced Services
CCTV	closed circuit television
CIA	Central Intelligence Agency
DBT	design basis threat
DOD	Department of Defense
DOE	Department of Energy
DHS	Department of Homeland Security
DS	Diplomatic Security
DTRA	Defense Threat Reduction Agency
FPS	Federal Protective Service
FSRM	Federal Security Risk Management
GPRA	Government Performance and Results Act of 1993
GSA	General Services Administration
HEPA	high-efficiency particulate air
HSPD-12	Homeland Security Presidential Directive Number 12
HSPD-7	Homeland Security Presidential Directive Number 7
IG	Inspector General
Interior	Department of the Interior
ISC	Interagency Security Committee
LROBP	Long-Range Overseas Buildings Plan
NAS	National Academy of Sciences
NPS	National Park Service
OBO	Overseas Buildings Operations
OLES	Office of Law Enforcement and Security
OMB	Office of Management and Budget
OPAP	Overseas Presence Advisory Panel
PDD	Presidential Decision Directive
PIN	personal identification number
PSP	Physical Security Professionals
State	Department of State
USPS	U.S. Postal Service
VA	Department of Veterans Affairs
WMD	weapons of mass destruction

Contents

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

November 30, 2004

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

The war on terrorism has made physical security for federal facilities a governmentwide concern. The federal government owns or leases hundreds of thousands of facilities, with the vast majority concentrated in the Departments of Defense (DOD), Veterans Affairs (VA), State (State), Energy (DOE), and the Interior (Interior); the General Services Administration (GSA); and the U.S. Postal Service (USPS). The makeup of these facilities reflects the diversity of agencies' missions and includes office buildings, military installations, hospitals, embassies, border stations, laboratories, and park visitor centers.

After the September 11, 2001, attacks, Congress passed the Homeland Security Act of 2002, which created the Department of Homeland Security (DHS). In creating DHS, the government's efforts to prevent, protect against, and respond to potential terrorism—including terrorism directed at federal facilities—were centralized. As a result of the act, DHS assumed responsibility for chairing the Interagency Security Committee (ISC). ISC, which has representation from all the major property-holding agencies and was established after the bombing of the Oklahoma City federal building, has a range of governmentwide responsibilities related to protecting nonmilitary facilities. These generally involve developing policies and standards, ensuring compliance and overseeing implementation, and sharing and maintaining information.[1] Although ISC was established to bring a central focus to the government's efforts and provide a forum for sharing key practices and lessons learned in protecting facilities, we reported in September 2002 that ISC was having limited success in fulfilling its responsibilities, because of the lack of consistent and aggressive leadership by GSA, inadequate staff support and funding for ISC, and ISC's difficulty in making decisions.[2]

[1]Presidential Executive Order 12977, Oct. 19, 1995.

[2]GAO, *Building Security: Interagency Security Committee Has Had Limited Success in Fulfilling Its Responsibilities*, GAO-02-1004 (Washington, D.C.: Sept. 17, 2002).

Our objectives were to (1) assess ISC's progress in fulfilling its responsibilities and (2) identify key practices in protecting federal facilities and any related implementation obstacles. To assess ISC's progress in fulfilling its responsibilities, we interviewed the Executive Director of ISC; analyzed ISC publications and other documents; considered prior GAO work; and reviewed various laws and policies, including the Homeland Security Act of 2002. We also reviewed the executive order that established ISC, a subsequent executive order that amended it in connection with the transfer of ISC's function to DHS, and relevant homeland security policy directives. To identify key practices, we systematically analyzed 170 GAO and Inspector General (IG) reports issued since 1995 that addressed homeland security and terrorism issues and pertained to facility protection. We also contracted with the National Academy of Sciences (NAS) to convene a symposium of experts on key practices in facility protection. Appendix II contains the symposium agenda and identifies the panelists. We also interviewed officials and analyzed documents from DHS and the major property-holding agencies, including DOD, VA, State, DOE, Interior, GSA, and USPS. For the purpose of this review, we defined key practices as those activities that, on the basis of our analysis, were recommended by GAO and others, acknowledged by agencies, and validated by experts in the area. More information on our scope and methodology appears in appendix I. We did our work from November 2003 through October 2004 in accordance with generally accepted government auditing standards.

Results in Brief

ISC has made progress in coordinating the government's facility protection efforts but faces certain challenges to fulfilling some of its major responsibilities. In recent years, ISC has taken several actions that relate to developing policies and guidance for facility protection. For example, ISC has updated its security design criteria for federal construction and developed guidance on security for federally leased space. ISC has also made progress related to sharing and maintaining information by, for example, developing a Web site and establishing standard operating procedures for ISC and its member agencies to follow for sharing information. Although its actions to ensure compliance and provide oversight, which were specified in the 1995 executive order, have been limited, in July 2004, the administration made ISC responsible for reviewing agencies' physical security plans that are required under a December 2003 presidential homeland security policy directive. Filling this role would represent a major step toward meeting its compliance and oversight responsibilities. Despite the overall progress ISC has made, and its prominent new role in the administration's oversight activities, it faces a

number of challenges. For example, the sheer magnitude of integrating the government's facility protection initiatives, which involves many different agencies and varying perspectives on security, is an ongoing, formidable task. Complicating this situation, significant resource constraints hinder ISC's ability to fulfill this and other related responsibilities. ISC has one full-time staff person and is dependent on participation from member agencies to fulfill its mission. In addition to these challenges, ISC lacks an action plan, which we are recommending, that could be used to (1) provide DHS and other stakeholders with detailed information on, and a rationale for, its resource needs; (2) garner and maintain the support of ISC member agencies, DHS management, Office of Management and Budget (OMB), and Congress; (3) identify implementation goals and measures for gauging progress in fulfilling all of its responsibilities; and (4) propose strategies for addressing the challenges ISC faces. Without an action plan, ISC's strategy and time line for implementing its responsibilities remain unclear. DHS concurred with this recommendation.

As ISC and agencies have paid greater attention to facility protection in recent years, several key practices have emerged that collectively could provide a framework for guiding agencies' efforts. These include allocating resources using risk management; leveraging security technology; sharing information and coordinating protection efforts with other stakeholders; measuring program performance and testing security initiatives; realigning real property assets to mission, thereby reducing vulnerabilities; and, implementing strategic human capital management, to ensure that agencies are well equipped to recruit and retain high-performing security professionals. More specifically, these key practices encompass the following:

- *Allocating resources using risk management*—A risk management approach to facility protection, which, for example, DOD has employed for several years to protect its critical facilities, involves identifying potential threats, assessing vulnerabilities, identifying the assets that are most critical to protect in terms of mission and significance, and evaluating mitigation alternatives for their likely effect on risk and their cost. Using information on these elements, a strategy for allocating security-related resources is developed, implemented, and reevaluated over time as conditions change.

- *Leveraging technology*—To address threats and vulnerabilities, leveraging technology—through supplementing other measures with technology in a cost-effective manner—enhances facility protection. For

example, advanced methods for screening access to facilities, such as smart cards that GSA is piloting in New York City, have been used to strengthen security. Smart cards use integrated circuit chips, which store information on individuals; and biometrics, which analyze human physical and behavioral characteristics. Sophisticated surveillance systems can also help secure building perimeters and monitor activity in the building.

- *Information sharing and coordination*—Establishing a means of coordinating and sharing information with other government entities and the private sector is crucial to prevent, protect against, and respond to potential terrorism. Facility managers are highly dependent on guidance and input from outside stakeholders to address threats directed at federal facilities. For example, DOE has memoranda of agreement in place with federal, state, and local law enforcement agencies and works with DOD to secure facilities that house the nation's nuclear stockpile.

- *Performance measurement and testing*—Performance measurement can be used to ensure accountability for achieving broad program goals and improved security at the individual building level. For broader program goals, measures could focus on implementation time lines and adherence to budgets. At the individual building level, active testing using, for example, on-site security assessments can provide data on the effectiveness of efforts to reduce vulnerabilities. Training exercises and drills are also useful in assessing preparedness.

- *Aligning assets to mission can reduce vulnerabilities*—The government's long-standing problem with excess and underutilized property has implications for facility protection. To the extent that agencies are expending resources to maintain and protect facilities that are not needed, realigning assets to mission and relocating staff can reduce vulnerabilities by reducing the number of assets that need to be protected. Furthermore, expending resources to protect unneeded facilities may reduce funds available to protect other more vulnerable facilities and staff. An example where this is occurring is State's attempt to "rightsize" its overseas presence, which gives heavy consideration to reducing security vulnerabilities as part of an asset realignment effort.

- *Strategic human capital management*—In facility protection, as with other areas pertaining to homeland security, it is especially critical for agencies to be well equipped to recruit and retain high-performing

security and law enforcement professionals. We have reported in recent years that overall, the government should take a strategic and results-oriented approach to managing and maintaining the human capital needed to maximize government performance and assure its accountability.

Although agencies have begun using these key practices to varying degrees, a number of implementation obstacles are apparent. These include developing quality data that form the basis for risk management, ensuring that technology will perform as expected, and determining how to measure the true impact that various approaches have on improving protection. Agencies also face significant, long-standing obstacles to realigning their facility portfolios and implementing human capital reforms in general. To help devise strategies for overcoming these obstacles and evaluate their efforts, agencies would benefit from having a set of key practices—such as those we have identified—that could be used to guide their efforts to protect facilities. We have advocated using guiding principles in other areas, including human capital management, information technology, and capital investment.[3] ISC, in serving as the central coordinator for agencies' efforts, is well positioned to promote key practices for facility protection and could consider using our work as a starting point. As such, we are recommending that the Chair of ISC pursue such an initiative and DHS concurred with this recommendation. Also, ISC member agencies including State, Interior, GSA, and DOE provided additional information and comments on a draft of this report, which we incorporated where appropriate.

Background

Terrorists have targeted federal facilities several times over the past 10 years. After the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the Department of Justice created minimum-security standards for federal facilities. In October 1995, the President signed Executive Order 12977, which established ISC. ISC was expected to enhance the quality and effectiveness of security in, and protection of,

[3]See GAO, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002); GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004); GAO, *Executive Guide: Leading Practices in Capital Decision-Making*, GAO/AIMD-99-32 (Washington, D.C.: December 1998); and GAO, *Information Technology: Training Can Be Enhanced by Greater Use of Leading Practices*, GAO-04-791 (Washington, D.C.: June 24, 2004).

facilities in the United States occupied by federal employees for nonmilitary activities and to provide a permanent body to address continuing governmentwide security issues for federal facilities. ISC is expected to have representation from all the major federal departments and agencies, as well as a number of key offices.[4] ISC's specific responsibilities under the executive order generally relate to three areas: developing policies and standards, ensuring compliance and overseeing implementation, and sharing and maintaining information. Related to policies and standards, the executive order specifically states that ISC is to

- establish policies for security in and protection of federal facilities;
- develop and evaluate security standards for federal facilities;
- assess technology and information systems as a means of providing cost-effective improvements to security in federal facilities;
- develop long-term construction standards for those locations with threat levels or missions that require blast-resistant structures or other specialized security requirements; and
- evaluate standards for the location of, and special security related to, day care centers in federal facilities.

In the area of compliance and oversight, ISC is to develop a strategy for ensuring compliance with facility security standards and oversee the implementation of appropriate security measures in federal facilities. And, related to sharing and maintaining information, ISC is to encourage agencies with security responsibilities to share security related intelligence in a timely and cooperative manner and assist with developing and maintaining a centralized security database of all federal facilities.

[4]ISC's membership includes the Departments of State, Treasury, Defense, Justice, the Interior, Agriculture, Commerce, Labor, Health and Human Services, Housing and Urban Development, Transportation, Energy, Education, and Veterans Affairs; GSA; the Environmental Protection Agency, Central Intelligence Agency (CIA), and OMB. Other members of ISC include the Director, U.S. Marshals Service and the Assistant to the President for National Security Affairs. As a member of ISC, DOD participates in meetings to ensure that DOD physical security policies are consistent with ISC security standards and policy guidance, according to the Executive Director of ISC.

Since September 11, the focus on protecting the nation's critical infrastructure has been heightened considerably. The Homeland Security Act of 2002 and other administration policies assigned DHS specific duties associated with coordinating the nation's efforts to protect critical infrastructure, and Homeland Security Presidential Directive Number 7 (HSPD-7) stated that DHS's Secretary was responsible for coordinating the overall national effort to identify, prioritize, and protect critical infrastructure and key resources.[5] Under the Homeland Security Act of 2002, the Federal Protective Service (FPS) was transferred from GSA to DHS and, as a result of this transfer, DHS assumed responsibility for ISC in March 2003.

In September 2002, we reported that ISC was having limited success in fulfilling its responsibilities.[6] Specifically, ISC had made little or no progress in areas including developing and establishing policies for security in and protection of federal facilities and developing a strategy for ensuring compliance with security standards. In January 2003, we designated federal property as a high-risk area, in part due to the threat of terrorism against federal facilities.[7] As the government's security efforts continue to intensify, and real property-holding agencies employ such measures as searching vehicles that enter federal facilities, restricting parking, and installing concrete bollards, important questions continue to be raised regarding the level of security needed to adequately protect federal facilities and how the security community should proceed. Figure 1 shows bollards installed at the Jacob Javits Federal Building in New York, New York. Additionally, questions concerning the cost-effectiveness and impact of various practices have emerged as the nation faces a protracted war on terrorism.

[5]Homeland Security Presidential Directive Number 7, *Critical Infrastructure Identification Prioritization, and Protection*, Dec. 17, 2003.

[6]GAO-02-1004.

[7]GAO, *High-Risk Series: Federal Real Property*, GAO-03-122 (Washington, D.C.: January 2003).

Figure 1: Bollards Installed at the Jacob Javits Federal Building

Source: GAO.

ISC Has Made Progress but Faces Challenges in Fulfilling Some of Its Major Responsibilities

ISC has made progress in coordinating the government's facility protection efforts and has been given a prominent role in reviewing agencies' physical security plans for the administration since we last reported on this issue. In September 2002, we reported that ISC, at that time, had made little or no progress in key elements of its responsibilities, such as developing policies and standards for security at federal facilities; ensuring compliance with security standards and overseeing the implementation of appropriate security in federal facilities; and related to information, developing a centralized security database of all federal facilities.[8] Agency representatives identified several factors that they believe contributed to

[8]GAO-02-1004.

ISC's limited progress. These factors included (1) the lack of consistent and aggressive leadership by GSA, (2) inadequate staff support and funding for ISC, and (3) ISC's difficulty in making decisions. Nonetheless, there were areas where we observed some progress over its then 7-year existence. For example, ISC had developed and issued security design criteria and minimum standards for building access procedures; disseminated information to member agencies on entry security technology for buildings needing the highest security levels; and, through its meetings and working groups, provided a forum for federal agencies to discuss security-related issues and share information and ideas.[9]

In commenting on the September 2002 report, GSA, which at the time had responsibility for chairing ISC, agreed to take action to address the shortcomings we identified. In March 2003, in accordance with the Homeland Security Act of 2002, FPS was transferred from GSA to DHS. As a result, DHS assumed responsibility for chairing ISC, and the executive order establishing ISC was amended to reflect the transfer of this function from GSA to DHS.[10] Transferring responsibility for ISC to DHS reflected the shift to having homeland security activities centralized under one cabinet-level department. Within DHS, the role of chairing ISC was subsequently delegated to the Director of FPS in January 2004.

Since our 2002 report, ISC has made clear progress in developing policies and standards and maintaining and sharing information. Related to policies and standards, ISC issued security standards for leased space in July 2003, and OMB has approved them. These standards address security requirements for leased facilities and, according to an ISC official, are currently being used by ISC member agencies as a management tool. In June 2003, ISC issued guidance on escape hoods for federal agencies and, in October 2003, ISC issued an update to its May 2001 *Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*. According to an FPS official, GSA is incorporating ISC's *Security Design Criteria* in the construction of new facilities. More recently, ISC became involved with Homeland Security Presidential Directive Number 12 (HSPD-12), issued in August 2004, which seeks to standardize identification

[9]GAO-02-1004.

[10]Presidential Executive Order 13286, Mar. 5, 2003.

for federal employees and contractors.[11] According to the directive, wide variations in the quality and security of forms of identification used to gain access to federal facilities, where there is a potential for terrorist attacks, need to be eliminated. ISC's Executive Director informed us that he was asked to be a member of the White House Homeland Security Council Coordination Committee for HSPD-12. This ISC official would provide the leadership role for this committee and ensure that physical security requirements for the federal government, as they relate to the directive, are included and coordinated with ISC members.

Related to its role in maintaining and sharing information, ISC has developed a Web site for posting policies and guidance and is developing a secure Web portal for member agencies to exchange security guidance and other information. Also, according to the Executive Director of ISC, standard operating procedures were approved by ISC members in June 2004 and were finalized in September 2004. These operating procedures are intended to improve the quality of information sharing among member agencies at its meetings by establishing standards for attendance and participation at ISC meetings. For example, each ISC agency representative is required to attend all meetings or delegate a person to attend to ensure full participation. Finally, DHS is developing a governmentwide facilities database that the ISC Executive Director believes will meet ISC's responsibility to assist with developing and maintaining a centralized security database of all federal facilities. This database will list functions and services that are mission critical, map federal assets and their critical infrastructure, and identify key resources for both cyber and physical security protection. According to ISC's Executive Director, ISC members are an integral part of this process and will ensure that the required support from within their departments and agencies is provided.

New Role Could Provide Vehicle for Addressing Responsibilities Related to Ensuring Compliance and Overseeing Implementation

Despite progress in its other areas of responsibility, ISC has not developed, as specified in its 1995 executive order, a strategy for ensuring compliance with security standards among agencies and overseeing the implementation of appropriate security measures in federal facilities. However, in July 2004, the administration made ISC responsible for annually reviewing and approving physical security plans that agencies are required to develop under a presidential homeland security policy

[11]Homeland Security Presidential Directive Number 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, Aug. 27, 2004.

directive. HSPD-7, issued in December 2003, establishes a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources in the United States so that they can be protected from terrorist attacks. The directive makes DHS responsible for overseeing the implementation of the directive and outlines the roles and responsibilities of individual agencies. Among the roles and responsibilities delineated, HSPD-7 establishes an annual reporting cycle for agencies to evaluate their critical infrastructure and key resources protection plans for both cyber and physical security. ISC's Executive Director informed us that in July 2004, the administration designated ISC as the oversight body for agencies' physical security plans. According to ISC's Executive Director, ISC's role will be to review, approve, or disapprove each department or agency's physical security plan.

If ISC were to successfully fulfill its new responsibilities under HSPD-7, which would be done under the broader umbrella of the administration's central planning and coordination efforts for homeland security, it would represent a major step toward meeting its responsibilities that relate to oversight and compliance monitoring, as specified in the 1995 executive order under which it was established. That is, the 1995 executive order that established ISC specified that ISC should develop a strategy for ensuring agencies' compliance with governmentwide facility protection standards and oversee the implementation of appropriate security measures in federal facilities. By having a role in reviewing agencies' physical security plans in relation to HSPD-7, ISC would have a vehicle for carrying out its existing responsibility related to compliance and oversight. Appendix III identifies each of ISC's major responsibilities under the executive order and actions it has taken to date to fulfill them.

ISC Faces Challenges to Fulfilling Its Responsibilities

ISC's Executive Director identified several challenges that relate to ISC's many roles and responsibilities in coordinating the government's facility protection efforts. These included the following:

- reaching a consensus with agencies on a risk management process for the government that is reasonable and obtaining funding for this activity;

- addressing the issue of leased government space and the impact that new physical security standards for leased space will have on the real estate market;

- developing a compliance process for agencies that can also be used as a self-assessment tool to measure the effectiveness of ISC;

- educating senior level staff from across the government and gaining their support for ISC activities; and overall,

- integrating all physical security initiatives for the entire federal government and implementing change.

We agree that ISC faces these challenges and, furthermore, that they will have to be addressed in order for ISC to be successful. More specifically, the sheer magnitude of integrating the government's facility protection initiatives, which ISC and FPS officials identified, is formidable because it involves many different agencies and varying perspectives on security. Furthermore, in discussing the challenges associated with leased property, ISC's Executive Director touched on one of several long-standing problems in the federal real property area that have implications for facility protection policy. As reported in GAO's 2003 high-risk report on federal real property, the government's historical reliance on costly leased space—which achieves short-term budget savings but is more costly over the longer term—is problematic. To the extent that private sector lessors are required to enhance the security of their property for federal tenants, the associated costs will likely be passed on to the government in the form of higher rent.

Another long-standing problem that could affect ISC as it attempts to meet its responsibilities is the historically unreliable nature of agency real property data. Poor data could make it difficult for agency management to implement and oversee comprehensive risk-based approaches to protecting their facilities. As discussed later, risk management, as it pertains to facility protection, relies heavily on accurate and timely data. At the governmentwide level, inventory data maintained by GSA for the entire government, and financial data on property reported in the government's financial statements, have also been historically unreliable.[12]

Another challenge identified by ISC's Executive Director—obtaining adequate resources for its activities—is a particular concern. According to

[12]See GAO-03-122 and GAO, *Fiscal Year 2003 U.S. Government Financial Statements: Sustained Improvement in Federal Financial Management Is Crucial to Addressing Our Nation's Future Fiscal Challenges*, GAO-04-886T (Washington, D.C.: July 8, 2004).

the Executive Director of ISC, as the ISC's only full-time staff person, his ability to ensure that all of ISC's responsibilities are fulfilled is limited. Also, according to this official, ISC is dependent entirely on participation and input from member agencies. ISC's Executive Director said that, in the past, getting buy-in and support from senior officials in member agencies had been a challenge. It seems, however, that given ISC's new role in the administration's homeland security efforts, it could make a persuasive case for a sustained level of support from agencies. Also, it is important to note that DHS has certain responsibilities under the executive order that established ISC to ensure it has adequate resources. Specifically, the executive order states that "to the extent permitted by law and subject to the availability of appropriations, the Secretary of Homeland Security should provide ISC with such administrative services, funds, facilities, staff, and other support services as may be necessary for the performance of its functions."[13] According to ISC's Executive Director, current ISC resources are not sufficient for ISC to meet all of its evolving responsibilities. This official told us that additional funding for ISC will not be available until fiscal year 2006. However, given the prominent role ISC will be playing in the administration's homeland security efforts, it will be critical for DHS to help ISC undertake activities that will allow it to fulfill its responsibilities, address other challenges it faces, and ultimately be successful.

Given the challenges ISC faces, its new responsibility related to HSPD-7 for reviewing agencies' physical security plans, and the need to sustain progress it has made in fulfilling its responsibilities, ISC would benefit from having a clearly defined action plan for achieving results. Although ISC has taken steps to address challenges, such as seeking additional resources for fiscal year 2006, it lacks an action plan that could be used to (1) provide DHS and other stakeholders with detailed information on, and a rationale for, its resource needs; (2) garner and maintain the support of ISC member agencies, DHS management, OMB, and Congress; (3) identify implementation goals and measures for gauging progress in fulfilling all of its responsibilities; and (4) propose strategies for addressing the challenges ISC faces. Such a plan could incorporate the strategy for ensuring compliance with facility protection standards that is required under ISC's

[13]Presidential Executive Order 12977, Oct. 19, 1995, originally stated that the Administrator of GSA would provide ISC administrative services, funds, facilities, staff, and other support services necessary for the performance of ISC functions. Executive Order 13286 amended Executive Order 12977 to reflect the transfer of ISC to DHS and substituted the Secretary of DHS for the Administrator of GSA.

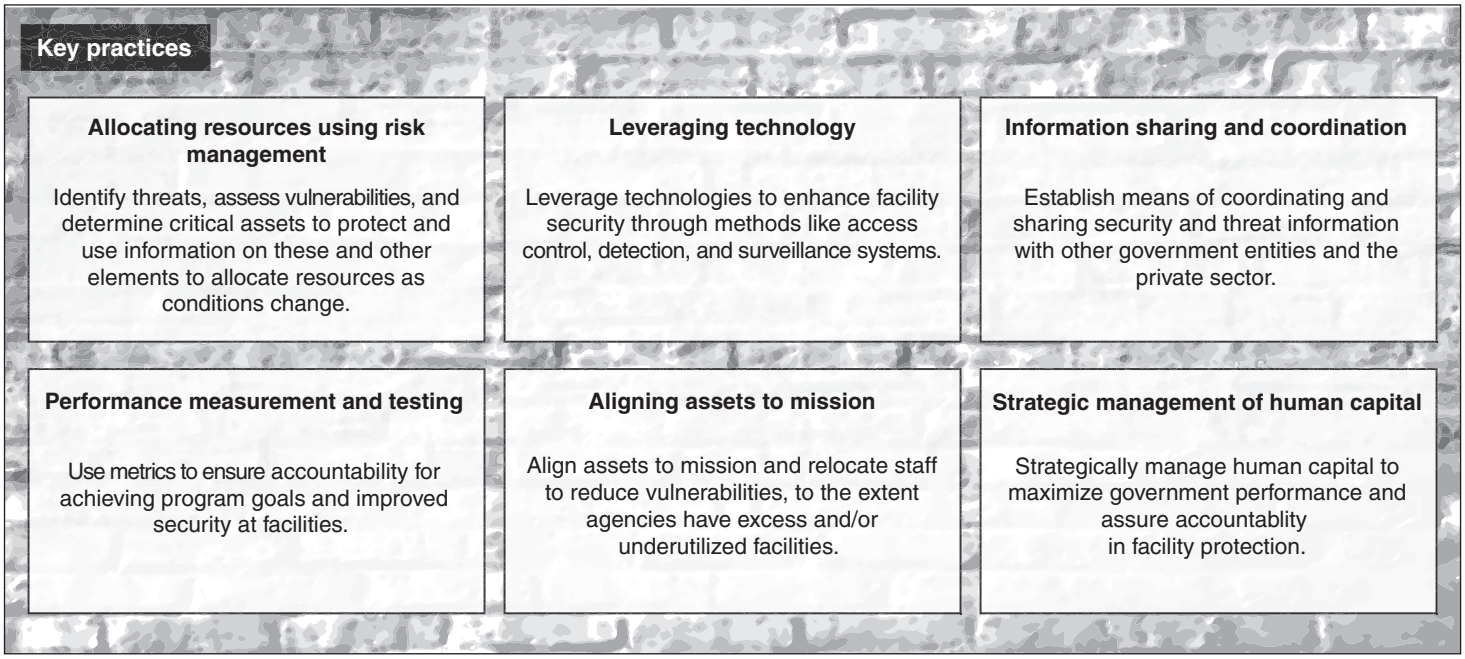
executive order, but has not yet been developed. Without an overall action plan for meeting this and other responsibilities, ISC's strategy and time line for these efforts remain unclear.

Having an effective ISC is critically important to the government's overall homeland security efforts as new threats emerge and agencies continue to focus on improving facility protection. Prior to 1995, there were no governmentwide standards for security at federal facilities and agencies' efforts to coordinate and share information needed improvement. Without standards and mechanisms for coordination, there were concerns about the vulnerability of federal facilities to acts of terrorism. As recently as August 2004, information from DHS showed that threats against high-profile facilities in the New York area and Washington, D.C., are still a major concern.

Key Practices in Federal Facility Protection

As ISC and agencies have paid greater attention to facility protection in recent years, several key practices have emerged that collectively could provide a framework for guiding agencies' efforts. As discussed in more detail later, ISC could play a vital role in promoting key practices in relation to its information sharing responsibilities. Key facility protection practices that we identified include allocating security resources using risk management, leveraging the use of security technology, coordinating protection efforts and sharing information with other stakeholders, and measuring program performance and testing security initiatives. In addition, we determined that two other practices GAO has highlighted as governmentwide issues also have implications for the facility protection area. These include realigning real property assets to agencies' missions, thereby reducing vulnerabilities, and strategic human capital management, to ensure that agencies are well equipped to recruit and retain high-performing security professionals. Our analysis—based on our work and Inspector General (IG) reports, the views of the NAS symposium experts in facility protection, and interviews with federal agencies—showed that attention to these key practices could provide a framework for guiding agencies' efforts and achieving success in the facility protection area. Figure 2 identifies each of these key practices.

Figure 2: Key Practices in Facility Protection



Source: GAO.

Using Risk Management Prioritizes Limited Security Resources

Allocating resources using risk management is a systematic and analytical process to consider the likelihood that a threat will endanger an asset (structure, individual, or function) and identify, evaluate, select, and implement actions that reduce the risk or mitigate the consequences of an event. Although applying risk management principles to facility protection can take on various forms, our past work showed that most risk management approaches generally involve identifying potential threats, assessing vulnerabilities, identifying the assets that are most critical to protect in terms of mission and significance, and evaluating mitigation alternatives for their likely effect on risk and their cost. These and other elements of a risk management approach are described in more detail in appendix IV. Our work showed that there was consensus in the security community—including GAO, IGs, agencies, national experts, and the private sector—that utilizing risk management practices provides the foundation for an effective facility protection program. For example, GAO has previously reported that for homeland security and information systems security, risk management can provide a sound foundation for

effective security whether the assets are information, operations, people, or federal facilities.[14] In fact, dozens of GAO and IG reports since September 11—which addressed efforts to protect facilities at several agencies including DOD, State, Interior, and GSA—discussed how risk management should be used to guide programs and better prepare for, and respond to, terrorism and other threats.[15] We have also recognized the benefits of risk management in determining how best to maximize the impact of limited resources.[16] At our March 2004 NAS symposium, there was general consensus among panelists that risk management is useful in guiding security decisions and that this approach should be pursued by federal agencies. Some of the NAS panelists commented:

"I am a supporter of risk-based methodologies. I see a lot of benefits from this approach. First, [agencies] can weigh the amount of risk reduction versus the cost of that reduction. Secondly, if [agencies] have a proven model, [they] can actually provide sound security. We have found time and time again, after a terrorist event, [there is a] knee-jerk reaction where people…don't necessarily add security but [instead] give the appearance of taking some action." – Navy official

"One of the key corollaries to [a] risk-assessment process is the determination of cost-effectiveness. That is a balancing act between the cost of the mitigation measures that we implement and the reductions in future losses, which we refer to as benefits." – Federal Emergency Management Agency official

"Threat assessments that we carry out are comparative, rather than absolute. By ranking the likelihood of a range of threats, in combination with a broad assessment of their potential consequences, we aim to show clients where their greatest risks lie by outlining proposals for mitigating these risks in the threat and risk assessment. The client can then prioritize how best to direct available resources." – Security consultant from the United Kingdom

Our discussions with the major property-holding agencies and analysis of documents we obtained showed that each agency used some form of risk management to protect its facilities. Some examples of how agencies applied risk management are as follows:

[14]GAO-02-687T.

[15]For example, see GAO, *Homeland Security: Critical Design and Implementation Issues*, GAO-02-957T (Washington, D.C.: July 17, 2002) and GAO, *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: Oct. 12, 2001).

[16]GAO, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001).

- According to officials with FPS, which protects federally owned or occupied facilities held by GSA and DHS, security needs and related countermeasures are prioritized based on the level of risk to a particular facility. Risk is determined by evaluating the impact of loss and vulnerability that each specific threat would have on a facility. According to these officials, FPS inspectors are trained to make educated decisions on applicable countermeasures to the identified threats and vulnerabilities on a recurring basis.

- We have reported that, for many years, DOE has employed risk-based security practices.[17] To manage potential risks, DOE uses a classified document referred to as a "design basis threat" (DBT). The DBT identifies the potential size and capabilities of terrorist forces and is based on information DOE gathers from the intelligence community. DOE requires contractors operating its sites to provide sufficient protective forces and equipment to defend against the threat contained in the DBT. DOE updated its 1999 DBT in May 2003 to better reflect current and projected terrorist threats in the aftermath of September 11.

- VA conducts physical security assessments and prioritizes its protection efforts for critical infrastructure, according to VA officials. The phases of the assessment include defining the criticality of VA facilities, identifying and analyzing vulnerabilities of VA's critical facilities, and identifying appropriate countermeasures. According to VA documents, VA determines vulnerability by factors such as facility population, number of floors in the facility, and the presence or absence of armed officers. This assessment also includes a procedure for scoring and prioritizing identified vulnerabilities at each assessed site.

- We have reported that DOD requires its installations to assess, identify, and evaluate potential threats to the installation; identify weaknesses and countermeasures to address the installation's vulnerabilities; and evaluate and rank criticality of the installation's assets to achieving mission goals.[18] These three assessments serve as the foundation of each DOD installation's antiterrorism plan. The results of the

[17]GAO, *Nuclear Security: Several Issues Could Impede the Ability of DOE's Office of Energy, Science and Environment to Meet the May 2003 Design Basis Threat*, GAO-04-894T (Washington, D.C.: June 22, 2004).

[18]GAO, *Homeland Security: Challenges and Strategies in Addressing Short-and-Long-Term National Needs*, GAO-02-160T (Washington, D.C.: Nov. 7, 2001).

assessments are used to balance threats and vulnerabilities and to define and prioritize related resource and operational requirements.

- Interior's Office of Law Enforcement and Security (OLES) has identified 16 Interior assets as needing special consideration because they are critical to the nation's infrastructure or are national icons that could be targets for symbolic reasons.[19] Having a rationale such as this, for focusing on certain assets, represents Interior's approach to risk management at the departmentwide level.

- According to USPS officials, USPS's physical security program incorporates a risk assessment methodology and a layered approach to facility security. This effort involves annual security surveys of facilities conducted by facility security control officers and periodic comprehensive reviews at larger core postal facilities by the Postal Inspection Service, which is the investigative branch of USPS.

- In commenting on this report, State noted that another example of an agency's use of risk management is State's Long-Range Overseas Buildings Plan (LROBP). LROBP is a 6-year plan, updated yearly, that identifies embassy and consulate facilities most in need of replacement due to unacceptable security, safety, and/or operational conditions. State also said that the plan identifies State's facilities' program objectives and prioritizes competing facility requirements with input from the Bureaus of Overseas Buildings Operations (OBO) and Diplomatic Security (DS), State's Regional Bureaus, and other overseas agencies. State indicated that the LROBP provides a road map for addressing long-term facility needs under the Capital Security Construction Program, Regular Capital Construction Program, as well as major rehabilitation, compound security, and other programs. According to State's comments, to prepare the plan, each year OBO and DS meet with the regional bureaus to discuss which posts should move into the "top 80" list, which contains the 80 primary posts requiring replacement for security reasons, and for which, by law, the department can spend security capital construction appropriations. Furthermore, with respect to the original full list of facilities that need replacement, the department, working with intelligence agencies, prioritizes these facilities.

[19]Interior officials requested that we not publicly identify these 16 assets because of security concerns.

At the NAS symposium, a private sector security expert discussed a risk management methodology in use by FPS at GSA and Internal Revenue Service facilities. We did not review the usefulness or effectiveness of this methodology. Nonetheless, the methodology is an example of one risk management process that is in use. The process, called Federal Security Risk Management, or FSRM, is a risk matrix that compares credible threats with assets and assesses the impact of loss and vulnerability. According to the panelist, agencies use the risk matrix to apply security upgrades to the risks deemed unacceptable and reevaluate the countermeasures until a desired level of risk reduction is achieved. The agencies then develop design or retrofit specifications and criteria. This risk assessment cycle generally spans a 2-to-4 year time period. According to the panelist, once unacceptable risks are addressed through countermeasures, agencies need to reevaluate risks and vulnerabilities on an ongoing basis.

Leveraging Security Technologies Can Enhance Facility Protection

By efficiently using technology to supplement and reinforce other security measures, vulnerabilities that are identified by the risk management process can be more effectively addressed with appropriate countermeasures. Our work showed broad concurrence among GAO, IGs, facility security experts, and agency experts that making efficient use of security technology to protect federal facilities is a key practice, but that the type of technology to use should be carefully analyzed. For example, in reporting on border security and information security issues in 2003, we found that prior to significant investment in a project, a detailed analysis should be conducted to determine that benefits of a technology outweigh costs, as well as to determine the effects of the technology on areas such as privacy and convenience.[20] In the facility access control area, we also reported that agencies should decide how technology will be used and whether to use technology at all to address vulnerabilities before implementation.[21] According to our 2003 testimony on using technologies to secure federal facilities, technology implementation costs can be high, particularly if significant infrastructure modifications are necessary.[22]

[20]GAO, *Border Security: Challenges in Implementing Border Technology*, GAO-03-546T (Washington, D.C.: Mar. 12, 2003); GAO, *Information Security: Challenges in Using Biometrics*, GAO-03-1137T (Washington, D.C.: Sept. 9, 2003).

[21]GAO-03-1137T.

[22]GAO, *Electronic Government: Challenges to the Adoption of Smart Card Technology*, GAO-03-1108T (Washington, D.C.: Sept. 9, 2003).

Another consideration is that lesser technological solutions sometimes may be more effective and less costly than more advanced technologies. For example, as we reported in 2002, trained dogs are an effective and time-proven tool for detecting concealed explosives. By using the risk management process and balancing costs, benefits, and other concerns, agencies can efficiently leverage technologies to enhance facility protection.

Among the advanced technologies that were identified during our review were smart cards—which use integrated circuit chips to store information on individuals—and biometrics—which analyze human physical and behavioral characteristics—to verify the identity of employees. Furthermore, sophisticated detection and surveillance systems such as closed circuit television (CCTV) have also aided in securing facility perimeters and monitoring activity in the building. Such technologies expand surveillance capabilities and can free up security staff for other duties. Several GAO and IG reports indicated that agencies currently have a wide array of security technologies available for protecting facilities, including smart cards, biometrics, X-ray scanners, and CCTV.[23] As we reported in 2002, technologies identified as countermeasures through the risk management process support the following three integral concepts for security:

- *Protection*—Provides countermeasures such as policies, procedures, and technical controls to defend assets against attacks.

- *Detection*—Monitors for potential breakdowns in protective mechanisms that could result in security breaches.

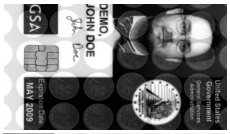
- *Reaction*—Responds to detected breaches to thwart attacks before damage can be done.

[23]For example, see GAO-03-1108T; GAO-03-1137T; GAO-03-546T; U.S Department of State, Office of Inspector General, *Limited-Scope Security Inspection of Embassy Port of Spain, Trinidad, and Tobago*, SIO-I-03-22, August 2003; U.S. Department of State, Office of Inspector General, *Security Inspection of Embassy N'Djamena, Chad*, SIO-I-03-27, June 2003; and U.S. Department of State, Office of Inspector General, *Security Inspection of Embassy Yaounde, Cameroon*, SIO-I-03-28, March 2003.

In GAO's April 2002 testimony on security technologies, we categorized the security technologies by which security concept they supported.[24] Figure 3 lists the technologies and provides descriptions of each.

Figure 3: Examples of Technologies Used in Facility Protection

Protection (access)



Smart cards
Smart cards are plastic devices about the size of a credit card that use integrated circuit chips to store and process data, much like a computer. Cards can store information such as color photos, multiple fingerprint images, or other digitized images as well as data to substantiate the card's authenticity and make it difficult to counterfeit. This processing capability distinguishes these cards from traditional magnetic strip cards, which cannot interact with automated information systems to securely exchange data.

Biometrics
Biometrics measure characteristics thought to be distinct to an individual. For personal identification, biometric technologies measure human physiological and behavioral characteristics. For example, biometric technologies take direct measurements of fingertips, hand and facial geometry, and retinas. Biometric technologies can also measure behavioral characteristics such as speech and signature unique to an individual.

Other access technologies
Other access technologies include keypad entry systems, which require users to enter passwords or PINs to gain access to facilities.

Detection and reaction

X-ray and explosive detection systems
Detection systems provide a second layer of security. X-ray scanning systems use electromagnetic waves (X-rays) to allow distinct structures to be viewed on a monitor. Items are distinguishable due to differences in material composition. Metal detectors are used to locate concealed metallic weapons. When the detector senses a questionable item or material, an alarm is signaled. Explosive detection systems can detect bulk or trace explosives concealed in, on, or under vehicles, containers, packages, and persons.

Intrusion detection
Intrusion detection or surveillance systems 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 addition, CCTV systems can include other functions such as zoom features, motion and infrared sensors, audio, and threshold alarms. Intrusion sensors can also be used in buildings to detect penetrations into secure areas through walls, roofs, doors, and windows.

Source: GAO.

[24] GAO-02-687T.

Several of the major property-holding agencies we contacted use various security technologies to protect their facilities. For example, to control access to its embassies, State employs alarm systems, arrest barriers to stop vehicles, audio/video monitoring equipment, explosive detection devices and metal detectors, and X-ray machines. Officials at USPS indicated that various detection technologies are used to secure its facilities against biological and radiological agents. For example, as we reported in 2002, USPS installed high-efficiency particulate air (HEPA) filtration systems at some facilities to protect them from biohazards.[25] HEPA filtering technology is designed to remove particulate biohazards and other particles.

Currently, GSA is conducting a smart card pilot program for two federal buildings in New York City. Although the first cards went into use in October 2003, planning for the pilot program began before the September 11 terrorist attacks. One of the federal buildings participating in the program is the Jacob Javits Federal Building, which houses approximately 35 agencies and more than 7,000 federal employees. All of the employees participating in the program use smart cards to enter the building. In addition to a person's name, title, and picture, the smart card contains multiple layers of data substantiating the card's authenticity and personal biometric data of the cardholder. Employees use the smart cards at access portals near the building's entrances (see fig. 4). After the portal has read the smart card and validated the user, glass doors swing apart to allow entry. If the threat level is raised under the homeland security advisory system, the building access technology requires additional security procedures (e.g., entering a personal identification number (PIN), matching a stored biometric record).[26] Although agencies' use of smart cards in the building has been optional, all of the agencies in the Javits building are currently participating in the pilot program, including the Federal Bureau of Investigation, the Small Business Administration, and the Department of Housing and Urban Development.

[25]GAO, *Diffuse Security Threats: USPS Air Filtration System Need More Testing and Cost Benefit Analysis before Implementation*, GAO-02-838 (Washington, D.C.: Aug. 22, 2002).

[26]As we reported in GAO, *Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange*, GAO-04-453R (Washington, D.C.: Feb. 26, 2004), the Homeland Security Advisory System is composed of five color-coded threat conditions, which represent levels of risk related to potential terror attack. Red is severe, orange high, yellow elevated, blue guarded, and green low.

Figure 4: Smart Card Access Portals at the Jacob Javits Federal Building Entrance

Source: GAO.

Overall, it was evident during our review that agencies are already using or experimenting with a range of technologies in their facility protection efforts. In terms of key practices, it is important to note that focusing on obtaining and implementing the latest technology is not necessarily a key practice by itself. Instead, having an approach that allows for cost-effectively leveraging technology to supplement and reinforce other measures would represent an advanced security approach in this area. Also, linking the chosen technology to countermeasures identified as part of the risk management process provides assurance that factors such as purpose, cost, and expected performance were addressed.

Information Sharing and Coordination among Federal Agencies and the Private Sector Can Help Agencies Better Protect Their Assets

Information sharing and coordination among organizations is crucial to producing comprehensive and practical approaches and solutions to address terrorist threats directed at federal facilities. Our work showed a broad consensus—on the basis of prior GAO and IG work and information from agencies and the private sector—that by having a process in place to obtain and share information on potential threats to federal facilities, agencies can better understand the risk they face and more effectively determine what preventive measures should be implemented. In considering the implications that information sharing and coordination have for facility protection efforts, it is useful to look at how this practice is being approached governmentwide, at the agency level, and at the individual facility level.

At the governmentwide level, DHS is expected to play a critical role in information sharing and coordination in most homeland security areas, including facility protection. In September 2003, we reported that information sharing was critical for DHS to meet its mission of preventing terrorist attacks in the United States, reducing vulnerability to terrorist attacks, and minimizing damage and assisting with recovery if attacks do occur.[27] In 2003, we also reported that to accomplish its mission, DHS needed to access, receive, and analyze law enforcement information, intelligence information, and other threat, incident, and vulnerability information from federal and nonfederal sources and analyze this information to identify and assess the nature and scope of terrorist threats. Furthermore, we reported that DHS should share information both internally and externally with agencies, law enforcement, and first responders.[28] As we testified in September 2003, we have made numerous recommendations to DHS to improve information sharing and coordination to accomplish its homeland security responsibilities. These recommendations involved, for example,

- incorporating existing information-sharing guidance contained in various national strategies and the information-sharing procedures required by the Homeland Security Act of 2002;

[27]GAO, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-1165T (Washington, D.C.: Sept. 17, 2003).

[28]GAO-03-1165T.

- establishing a clearinghouse to coordinate the various information-sharing initiatives to eliminate possible confusion and duplication of effort;

- fully integrating states and cities into a national policy-making process for information sharing and taking steps to provide greater assurance that actions at all levels of government are mutually reinforcing;

- identifying and addressing perceived barriers to federal information-sharing; and

- using survey methods or related data collection approaches to determine, over time, the needs of private and public organizations for information related to homeland security and to measure progress in improving information sharing at all levels of government.[29]

In addition to those recommendations, we identified a need for a comprehensive plan to facilitate information sharing and coordination to protect critical infrastructure in our August 2004 testimony on strengthening information sharing for homeland security.[30] We reported that such a plan could encourage improved information sharing by clearly delineating roles and responsibilities of federal and nonfederal entities, defining interim objectives and milestones, setting time frames for achieving objectives, and establishing performance measures. DHS has concurred with the above recommendations to improve information sharing and coordination and is in various stages of implementing them. These recommendations clearly have implications for the facility protection area, by, for example, increasing coordination among facility stakeholders that would reduce duplicative efforts and reinforce protection strategies.

The emphasis on information sharing and coordination is also evident in the *National Strategy for Homeland Security* and its related strategies to protect critical infrastructure, including federal facilities. According to the national strategy, successfully protecting facilities will rely on effective information sharing and coordination among multiple entities as part of the

[29]GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: Aug. 27, 2003).

[30]GAO, *9/11 Commission Report: Reorganization, Transformation, and Information Sharing*, GAO-04-1033T (Washington, D.C.: Aug. 3, 2004).

nation's broader homeland security efforts. In the related *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, information sharing is a common theme. This strategy calls for the federal government to work with various stakeholders to, among other things, develop processes for visitor screening, assess vulnerabilities, develop construction standards, and implement security technology. With regard to national icon protection, the strategy recommends that Interior work with other agencies, the public, and the private sector to define criticality criteria, assess vulnerabilities, conduct security awareness programs, and collaborate to protect national icons outside the purview of the federal government. Related to dams, the strategy recommends that DHS work with other agencies, dam owners, and local and state officials to assess risks and institute a national dam security program.

At the agency level, the agencies we contacted provided several examples of their activities related to information sharing and coordination. These activities are described in table 1.

Table 1: Examples of Information Sharing and Coordination Identified by Agencies

Agency	Examples of coordinating agencies and organizations	Examples of information sharing activities
Department of Defense	Agencies: DHS and DOE, other federal entities Other organizations: state and local entities	• DOD requires commanders to form threat working groups with external law enforcement officials. • DOD's Defense Threat Reduction Agency (DTRA) shares responsibility for maintaining the U.S. nuclear weapon stockpile. • DTRA assists civilian agencies in antiterrorist programs such as first-responder training and addressing weapons of mass destruction threats.
Department of Energy	Agencies: DOD, DHS, federal law enforcement agencies Other organizations: state and local officials, law enforcement, and private sector	• Assigns personnel to serve as a central point of coordination and liaison with outside groups. • Some DOE facilities have entered into formal Memoranda of Agreements with other law enforcement agencies. • Directs sites to have formal or informal relationships with other federal, state, local, and private sector officials to address facility protection. • Works with DOD to secure U.S. nuclear weapons stockpile.
Department of State	Agencies: DHS, Environmental Protection Agency, GSA, Central Intelligence Agency, FBI, and various federal law enforcement agencies Other organizations: National Capital Planning Commission, the D.C. government	• Shares information through meetings, working groups, and joint projects. • GSA installs and maintains security systems for State's domestic facilities outside of the national capital region.

(Continued From Previous Page)

Agency	Examples of coordinating agencies and organizations	Examples of information sharing activities
Department of Homeland Security	Agencies: FBI, State, GSA tenant agencies, other federal law enforcement agencies Other organizations: private sector organizations with an interest in critical infrastructure protection	• As central coordinator of federal homeland security efforts, assists agencies with gathering facility threat information and incorporates it into risk assessments. • DHS, through FPS, provides tenant agencies with facility security assessments, containing threat and countermeasure information, and associated costs.
Department of the Interior	Agencies: DHS, DOD, FBI Other organizations: state and local government organizations, private sector	• Office of Law Enforcement and Security (OLES) serves as principal point of contact with external law enforcement and security organizations. • OLES is responsible for coordinating security policies and information sharing among Interior's bureaus, which collectively hold approximately 8,000 facilities.
Department of Veterans Affairs	Agencies: FEMA, DHS Other organizations: local law enforcement, public and private technical organizations	• VA facilities have entered into information sharing agreements and memoranda of understanding with local law enforcement. • Some VA officials participate in local law enforcement and public security councils to develop effective coordination and information sharing relationships.
General Services Administration	Agencies: DHS, tenants include most federal agencies Other organizations: local officials and law enforcement	• Participates in local and national public safety conferences to learn latest security information in the public and private sectors, and present information to others. These include conferences organized by, for example, the International Association of Chiefs of Police.
United States Postal Service	Agencies: DHS, GSA Other organizations: Legislative Task Force on Mail Safety	• Informs other agencies of mail and facility security issues.

Source: GAO.

In addition to agencywide efforts, coordination and information sharing is important at the individual facility level. As we have previously reported, protecting federal facilities requires facility security managers to involve multiple organizations to effectively coordinate and share information to prevent, detect, and respond to terrorist attacks.[31] Security managers typically are not aware of potential threats to their facilities and depend on intelligence from other organizations to prevent and/or deter attacks. For example, according to officials from VA, due to limited resources and its lack of an intelligence gathering capability, VA must rely on other agencies to gain threat information. Additionally, security managers have to coordinate and share information with state and local governments to

[31]GAO-02-687T.

respond to terrorist attacks and do not have direct access to the range of emergency resources required to respond to terrorist attacks. They rely on state and local governments to provide first-responder services such as firefighting, medical personnel, and other emergency services. They also rely on local police and the judicial process to enforce and prosecute violators of the laws and regulations governing the protection of federal facilities. As such, at the individual facility level, security managers are less equipped to make informed decisions about security without effective information sharing and coordination.

One way managers at the individual facility level may become better informed is if they take advantage of emerging efforts by the government to disseminate targeted threat information. For example, one recent DHS effort to increase information sharing and coordination among security stakeholders is its Homeland Security Information Network. According to DHS's Web site, this unclassified network consists of Internet, phone, fax, and pager communications systems that provides DHS with constant access to real-time threat information from public and private industries and agencies. DHS can also use the network to send targeted alert notifications and other threat information to states, cities, and others, which can then collect and disseminate this information among those other entities involved in combating terrorism. A base of locally knowledgeable experts governs and administers the network with the support of DHS regional coordinators.

Overall, IG reports and experts from the NAS symposium we held underscored the value of information sharing and coordination for facility protection. Regarding Interior's protection of national icons, Interior's IG has reported that coordination and communication are two key characteristics of any well-functioning organization.[32] State's IG has recommended that some embassies coordinate with local police to establish coordinated response procedures to potential vehicle bomb attacks.[33] State concurred with these recommendations. In a 2002 report, the GSA IG reported on the value of having security officials share any

[32]U.S. Department of the Interior, Office of Inspector General, *Review of National Icon Park Security*, 2003-I-0063 (Washington, D.C.: Aug. 28, 2003).

[33]U.S. Department of State, Office of Inspector General, *Security Inspection: Embassy Ljubljana, Slovenia*, SIO-I-03-03 (Washington, D.C.: November 2002).

gained expertise to address emerging threats to federal facilities.[34] At the NAS symposium, there was a general consensus among panelists that coordination and information sharing—whether through formal or informal means—is critical to effectively protect federal facilities. Some examples of panelist comments included:

"We should be sharing what we know. There are a limited number of people in this field…One thing we do need, to help us share this information, is more engineering forums, more opportunities for other federal agencies and the private sector to share… this information."—Defense official

"Whatever information sharing structure gets superimposed on agencies, it should not impede existing groups that share security information. Informal networks rather than rigid hierarchies are the things you really need to secure properties. In general, frequent interaction helps build trust, helping people to work together and respond quickly to threats."—Private sector security consultant

Performance Measurement Can Ensure Accountability for Achieving Broad Program Goals and Improved Security

Performance measurement can help achieve broad program goals and improve security at the individual facility level. Our analysis showed a consensus among various stakeholders that performance measurement is a key practice that agencies should follow. Although using performance measurement for facility protection is a practice that—based on our analysis—is in the early stages of development, several initiatives at three levels—governmentwide policy, agency, and facility-specific—demonstrate how performance measurement is being approached in the facility protection area.

At the governmentwide policy level, the *National Strategy for Homeland Security* addresses the threat of terrorism in the United States by organizing the domestic efforts of federal, state, local and private organizations.[35] It aligns and focuses homeland security functions into six mission critical areas, set forth as (1) intelligence and warning, (2) border and transportation security, (3) domestic counterterrorism, (4) protecting critical infrastructures and key assets, (5) defending against catastrophic terrorism, and (6) emergency preparedness and response. As mentioned before in relation to information sharing and coordination, the *National*

[34]General Services Administration, Office of Inspector General, *Audit of the Federal Protective Service's Federal Security Risk Manager Program*, A010129/P/2/R02007 (Arlington, VA: Mar. 27, 2002).

[35]Office of Homeland Security, *The National Strategy for Homeland Security*, July 2002.

Strategy for the Physical Protection of Critical Infrastructures and Key Assets[36] incorporates facility protection efforts and identifies a set of national goals and objectives. The strategy outlines the guiding principles that will underpin the government's efforts to secure the infrastructures and assets vital to national security, governance, public health and safety, the economy, and public confidence. It also provides a unifying organizational structure and identifies specific initiatives to drive the government's near-term national protection priorities and inform the resource allocation process. According to the strategy, the strategic objectives that underpin our national critical infrastructure and key asset protection effort include the following:

- identifying and assuring the protection of those infrastructures and assets that are deemed most critical in terms of national-level public health and safety, governance, economic and national security, and public confidence consequences;

- providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat; and

- assuring the protection of other infrastructures and assets that may become terrorist targets over time by pursuing specific initiatives and enabling a collaborative environment in which federal, state, and local governments and the private sector can better protect the infrastructures and assets they control.

These strategies are national in scope, cutting across all levels of government, and involve a large number of organizations and entities including federal, state, local, and private sectors. We have testified that these national strategies are the starting point for federal agencies and that the ultimate measure of this and other strategies' value will be the extent they are useful as guidance for policy and decision makers in allocating resources.[37] Related to facility protection, the strategic objectives are useful in providing a context and a broader framework for agencies, as they develop agencywide and facility-specific goals and measures to determine if their specific facility protection efforts are achieving desired results.

[36]Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003.

[37]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

Security Goals Can Be Tied to Broader Agency Mission Goals

At the agency level, we have reported that tying security goals to broader agency mission goals can help federal agencies measure the effectiveness and ensure accountability of their security programs.[38] One tool that agencies can use is the Government Performance and Results Act of 1993 (GPRA). Under GPRA, agencies are to prepare 5-year strategic plans that set the general direction for their efforts. These plans are to include comprehensive mission statements, general and outcome-related goals, descriptions of how those goals will be achieved, identification of external factors that could affect progress, and a description of how performance will be evaluated. Agencies are to then prepare annual performance plans that establish connections between the long-term goals in the strategic plans with the day-to-day activities of program managers and staff. These plans are to include measurable goals and objectives to be achieved by a program activity, descriptions of the resources needed to meet these goals, and a description of the methods used to verify and validate measured values. Finally, GPRA requires that the agency report annually on the extent to which it is meeting its goals and the actions needed to achieve or modify those goals that were not met.

GPRA provides a framework under which agencies can identify implementation time lines for facility protection initiatives and adherence to related budgets. We did not assess the extent to which agencies were using GPRA to develop agencywide facility protection or security-related goals. However, we noted one agency that ties its strategic security goals to GPRA is the Defense Threat Reduction Agency (DTRA) at DOD. DTRA's 2003 strategic plan contains most of the elements in a strategic plan developed using GPRA standards.[39] DTRA plays a key role in addressing the threats posed by weapons of mass destruction[40] (WMD), and its specialized capabilities and services are used to support civilian agencies' efforts to address WMD threats, particularly the efforts of DOE and DHS. DTRA also provides training for emergency personnel responding to WMD incidents and assesses the vulnerability of personnel and facilities to WMD threats.

[38]GAO, *Weapons of Mass Destruction: Defense Threat Reduction Agency Addresses Broad Range of Threats, but Performance Reporting Can Be Improved*, GAO-04-330 (Washington, D.C.: Feb. 13, 2004).

[39]GAO-04-330.

[40]WMD, once defined by DOD as nuclear, biological, and chemical, now includes radiological and high explosives as well.

DTRA's strategic plan lays out the agency's five goals, which serve as the basis of its individual units' annual performance plans: (1) deter the use and reduce the impact of WMD, (2) reduce the present threat, (3) prepare for future threats, (4) conduct the right programs in the best manner, and (5) develop people and enable them to succeed. These long-term goals are further broken down into four or five objectives, each with a number of measurable tasks under each objective. These tasks have projected completion dates and identify the DTRA unit responsible for the specific task. For example, under the goal "deter the use and reduce the impact of WMD" is the objective "support the nuclear force." A measurable task under this objective is to work with DOE to develop support plans for potential resumption of underground nuclear weapons effects testing. The technology development unit in DTRA was expected to complete this task by the fourth quarter of fiscal year 2004.

At the Individual Facility Level, Active Testing and Drills Can Help Gauge the Adequacy of Facility Protection

Our work showed examples where federal agencies were testing security measures by conducting inspections and assessments to ensure that adequate levels of protection are employed. For example, officials at Interior said that after September 11, one of its bureaus began conducting full-risk assessments at all of its facilities, in order of importance. As part of one of its regularly scheduled assessments at one location, Interior received assistance from DTRA, which performed an assessment of vulnerabilities. According to Interior officials, DTRA officials looked at whether the resulting effect from various types of attack would affect the mission capabilities of the location. After the assessment, DTRA made recommendations to Interior officials for strengthening security. Consequently, Interior officials took actions to improve security and scheduled plans for follow-up.

In another example, the Interior IG reported in August 2003 on its security assessment of National Park Service (NPS) parks. During the review, Interior IG officials identified some serious deficiencies with the overall security program and made recommendations to remedy these problems.[41] For example, the IG's assessment revealed that necessary security enhancements were delayed or wholly disregarded, that management officials lacked situational awareness, and that other officials lacked the expertise and resources to effectively assess, determine, and prioritize

[41]U.S. Department of the Interior, Office of Inspector General, *Review of National Icon Park Security*, 2003-I-0063 (Washington, D.C.: August 2003).

necessary security actions. This type of active testing is useful in exposing vulnerabilities and developing countermeasures.

According to DOE officials, DOE's Performance Assurance Program requires that performance testing determine the effectiveness of facility protection systems and programs. DOE conducts inspections to ensure that proper levels of protection are consistent with standards it has established. Assessments are made of the sites' ability to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contract employees, the public, or the environment. The adequacy of safeguards and security measures are then validated through various means such as surveys, periodic facility self-assessments, program reviews and inspections, and assessments.

In addition to testing facility access control through inspections and site surveys, we found examples of security programs that tested the effectiveness of physical security measures such as structural enhancements, physical barriers, and blast-resistant windows. Blast-resistance in buildings is generally provided by passive features such as additional reinforcement and connections in the structural frame for increased malleability, composite fiber wraps to prevent shattering of columns and slabs, and high-performance glazing materials that resist blast pressures. In both field tests and experience (for example, the attack on the Pentagon), these measures have been quite effective in reducing the devastating effects of deliberate explosions and, consequently, reducing casualties as well.

In March 2004, a panelist from DOD at the NAS symposium indicated that blast testing is also important in the prevention of injuries resulting from progressive collapse of buildings and flying debris. He reported that 87 percent of the deaths occurred in the collapsed portion of the Alfred P. Murrah Federal Building in Oklahoma City, and only 5 percent of the deaths occurred in the uncollapsed portion of the building. Furthermore, another panelist noted that 70 of the over 2,000 publicly reported terrorist incidents worldwide, since 1970, were directed at buildings. Most of these have involved large vehicle bombs, incendiary bombs, or rocket-propelled grenades.

Training exercises and drills are also useful in assessing preparedness. We have reported that effective security also entails having a well-trained staff

that follows and enforces policies and procedures.[42] In these reports, we found breaches in security resulting from human error are more likely to occur if personnel do not understand the technologies, risks, and the policies that are put in place to mitigate them. Furthermore, good training and practice are essential to successfully implementing policies by ensuring that personnel exercise good judgment in following security procedures. Presidential Decision Directive (PDD) 39[43] requires key federal agencies to maintain well-exercised capabilities for combating terrorism. Exercises test and validate policies and procedures, test the effectiveness of response capabilities, increase the confidence and skill levels of personnel, and identify strengths and weaknesses in responses before they arise in actual incidents. Counterterrorism exercises also include activities where agency officials discuss scenarios around a table or other similar setting, and field exercises, where agency leadership and operational units actually deploy to practice their skills and coordination in a realistic field setting.[44] Overall, training, as it relates to facility protection, provides decision makers with data on performance in various scenarios. Training is also discussed later in this report in relation to strategic human capital management.

Aligning Assets to Mission Can Reduce Security Vulnerabilities

Excess and underutilized real property at federal agencies is a long-standing and pervasive problem that has implications for the facility protection area. Along with the need to secure facilities against the threat of terrorism, excess property and the need to realign the federal real property inventory were among the reasons GAO designated federal real property as a high-risk area in January 2003.[45] To the extent that agencies are expending resources to maintain and protect facilities that are not needed, funds available to protect critical assets may be lessened. Our past work showed examples where funds spent to maintain and protect excess

[42]GAO-02-687T, and GAO, *Information Security: Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C.: Mar. 9, 2004).

[43]After the bombing of a federal building in Oklahoma City, Oklahoma, the President issued PDD 39 in June 1995, which enumerated responsibilities for federal agencies in combating terrorism, including domestic incidents. In May 1998, the President issued PDD 62 that reaffirmed PDD 39 and further articulated responsibilities for specific agencies.

[44]GAO, *Combating Terrorism: Analysis of Federal Counterterrorist Exercises*, GAO/NSIAD-99-157BR (Washington, D.C.: June 25, 1999).

[45]GAO-03-122.

property were significant. For example, we reported in January 2003 that DOD estimates it is spending $3 billion to $4 billion each year maintaining facilities that are not needed. In another example, costs associated with excess DOE facilities, primarily for security and maintenance, were estimated by the DOE IG in April 2002 to exceed $70 million annually.[46] One building that illustrates this problem is the former Chicago main post office. In October 2003, we testified that this building, a massive 2.5 million square foot structure located near the Sears Tower, is vacant and costing USPS $2 million annually in holding costs.[47] It is likely that other agencies that continue to hold excess or underutilized property are also incurring significant holding costs for services including security and maintenance.

Given the need to realign the federal real property inventory so that it better reflects agencies' missions, agencies that can overcome this problem may reap benefits in the facility protection area. That is, funds no longer spent securing and maintaining excess property could be put to other uses, such as enhancing protection at critical assets that are tied to agencies' missions. VA's Capital Asset Realignment for Enhanced Services (CARES) initiative, which VA started in October 2000, is an example where a realignment effort is under way. In the mid-1990s, VA began shifting its role from being a traditional hospital-based provider of medical services to an integrated delivery system that emphasizes a full continuum of care with a significant shift from inpatient to outpatient services. Subsequently, VA began the CARES initiative so that it could reduce its large inventory of buildings, many of which are underutilized or vacant.

"Rightsizing" the Overseas Presence

The administration's effort to "rightsize" the nation's overseas presence demonstrates how giving consideration to security, people, and facilities could be approached as part of an asset realignment framework. During 2000, an interagency effort led by the Department of State began to assess staffing of U.S. embassies and consulates to determine whether there were opportunities to improve mission effectiveness and reduce security vulnerabilities and costs by relocating staff. This process, referred to as rightsizing, was initiated in response to the November 1999

[46]DOE Office of the Inspector General, *Disposition of the Department's Excess Facilities*, DOE/IG-0550 (Washington, D.C.: Apr. 3, 2002).

[47]GAO, *Federal Real Property: Actions Needed to Address Long-standing and Complex Problems*, GAO-04-119T (Washington, D.C.: Oct. 1, 2003).

recommendations of the Overseas Presence Advisory Panel (OPAP).[48] In the aftermath of the August 1998 bombings of U.S. embassies in Africa, OPAP determined that overseas staffing levels had not been adjusted to reflect the changing missions and requirements; thus, some embassies and consulates were overstaffed, and some were understaffed. The framework provides a systematic approach for assessing workforce size and identifying options for rightsizing, both at the embassy level and for making related decisions worldwide. It links staffing levels to three critical elements of overseas diplomatic operations: (1) physical/technical security of facilities and employees, (2) mission priorities and requirements, and (3) cost of operations.

The first element includes analyzing the security of embassy buildings, the use of existing secure space, and the vulnerabilities of staff to terrorist attack. The second element focuses on assessing embassy priorities and the staff's workload requirements. The third element involves developing and consolidating cost information from all agencies at a particular embassy to permit cost-based decision making. Unlike an analysis that considers the elements in isolation, the rightsizing framework encourages consideration of a full range of options, along with the security, mission, and cost trade-offs. With this information, decision makers would then be in a position to, for example, determine whether rightsizing actions are needed either to add staff, reduce staff, or change the staff mix at an embassy. Options for reducing staff could include outsourcing functions or relocating functions to the United States or to regional centers. In May 2002, we testified that the use of this approach for the U.S. embassy in Paris was successful in identifying security concerns and finding alternative locations for staff, such as in the United States or other cities in Europe.[49] In April 2003, we reported that the rightsizing framework could be applied at U.S. embassies in developing countries.[50] We later testified in April 2003 that OMB should expand the use of the rightsizing framework and that

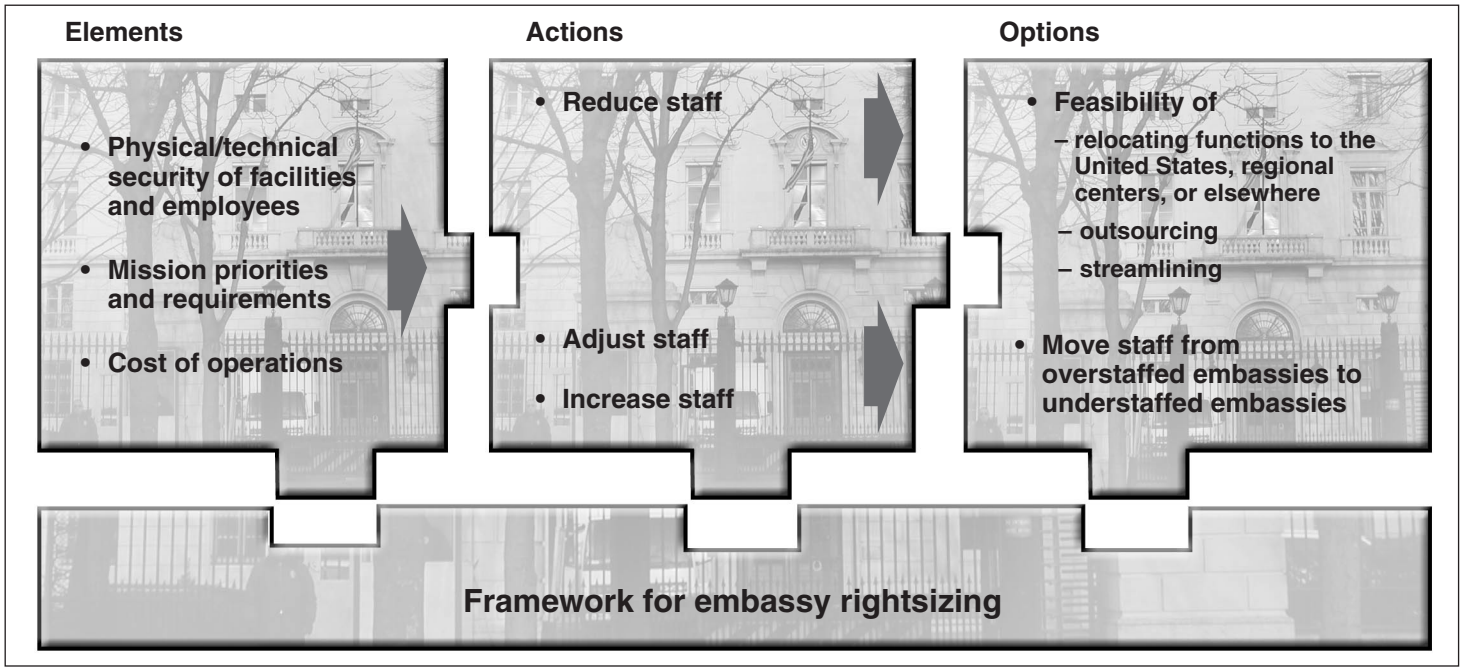
[48]State established OPAP following the 1998 embassy bombings in Africa and in response to recommendations of the Accountability Review Boards to consider the organization of U.S. embassies and consulates. Department of State, *America's Overseas Presence in the 21st Century, The Report of the Overseas Presence Advisory Panel* (Washington, D.C.: November 1999).

[49]GAO, *Overseas Presence: Observations on a Rightsizing Framework*, GAO-02-659T (Washington, D.C.: May 1, 2002).

[50]GAO, *Overseas Presence: Rightsizing Framework Can Be Applied at U.S. Diplomatic Posts in Developing Countries*, GAO-03-396 (Washington, D.C.: Apr. 7, 2003).

State adopt additional measures to ensure that U.S. agencies take a systematic approach to assessing workforce size that considers security, mission, and cost factors. GAO also recommended that State develop guidance on a systematic approach for developing and vetting staffing projections for new diplomatic compounds.[51] State and OMB agreed with our recommendations. Figure 5 illustrates the rightsizing process, which integrates security, people, and mission considerations in determining how facilities are used.

Figure 5: Framework for Embassy Rightsizing



Source: GAO.

[51]GAO, *Overseas Presence: Systematic Processes Needed to Rightsize Posts and Guide Embassy Construction*, GAO-03-582T (Washington, D.C.: Apr. 7, 2003).

Strategic Management of Human Capital Can Enhance Agency Facility Protection Efforts

The strategic management of human capital is a key practice that can maximize the government's performance and ensure the accountability of its efforts related to homeland security. People define an organization's culture, drive its performance, and embody its knowledge base. They are the source of all knowledge, process improvement, and technological advancements. As the government's homeland security efforts evolve, federal agencies involved with the intelligence community and other homeland security organizations will need the most effective human capital systems to reach projected security goals.[52] For facility protection, as with other areas related to homeland security, it is especially critical for agencies to recognize the "people" element and implement strategies to help individuals maximize their full potential. Also, it is important for agencies to be well equipped to recruit and retain high-performing security and law enforcement professionals. Training is also essential to successfully implementing policies by ensuring that personnel are well exercised and exhibit good judgment in following security procedures.

As we have reported, high-performing organizations align human capital approaches with missions and goals, and human capital strategies are designed, implemented, and assessed based on their ability to achieve results and contribute to an organization's mission.[53] This includes aligning their strategic planning and key institutional performance with unit and individual performance management, as well as implementing reward systems. We reported in March 2003 that federal agencies can develop effective performance management systems by implementing a selected, generally consistent, set of key practices.[54] These key practices helped public sector organizations both in the United States and abroad create a clear linkage or "line of sight" between individual performance and organizational success and, thus, transform their cultures to be more results-oriented, customer-focused, and collaborative in nature. These key practices, which have applicability to agencies' management of facility protection employers and contractors, include the following:

[52]GAO-04-1033T.

[53]GAO, *Results-Oriented Government: Shaping the Government to Meet 21st Century Challenges*, GAO-03-1168T (Washington, D.C.: Sept. 17, 2003).

[54]GAO, *Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success*, GAO-03-488 (Washington, D.C.: Mar. 14, 2003).

- *Align individual performance expectations with organizational goals*. An explicit alignment helps individuals see the connection between their daily activities and organizational goals.

- *Connect performance expectations to crosscutting goals***.** Placing an emphasis on collaboration, interaction, and teamwork across organizational boundaries helps strengthen accountability for results.

- *Provide and routinely use performance information to track organizational priorities***.** Individuals use performance information to manage during the year, identify performance gaps, and pinpoint improvement opportunities.

- *Require follow-up actions to address organizational priorities.* By requiring and tracking follow-up actions on performance gaps, organizations underscore the importance of holding individuals accountable for making progress on their priorities.

- *Use competencies to provide a fuller assessment of performance***.** Competencies define the skills and supporting behaviors that individuals need to effectively contribute to organizational results.

- *Link pay to individual and organizational performance.* Pay, incentive, and reward systems that link employee knowledge, skills, and contributions to organizational results are based on valid, reliable, and transparent performance management systems with adequate safeguards.

- *Make meaningful distinctions in performance***.** Effective performance management systems strive to provide candid and constructive feedback and the necessary objective information and documentation to reward top performers and deal with poor performers.

- *Involve employees and stakeholders to gain ownership of performance management systems*. Early and direct involvement helps increase employees' and stakeholders' understanding and ownership of the system and belief in its fairness.

- *Maintain continuity during transitions*. Because cultural transformations take time, performance management systems reinforce accountability for change management and other organizational goals.

Our analysis showed that several GAO and IG reports discuss the importance of strategic management of human capital in relation to homeland security functions, including facility protection. For example, in June 2004 we recommended that DHS develop a transformation strategy for FPS to resolve challenges related to, among other things, the change in organizational culture and responsibilities FPS faces since it was transferred from GSA to DHS.[55] DHS concurred with our recommendations. Furthermore, we testified on the importance of making changes to human capital management related to improving intelligence gathering at the CIA for security purposes.[56] Also, the DOE IG recommended that DOE standardize annual, refresher training requirements for security forces and conduct reviews of safeguards and security training programs departmentwide to ensure compliance with the agency training plan.[57] The Director, Office of Safeguards and Security at DOE, agreed with the recommendation.

Successfully training employees on using emerging security technologies is also an important element in facility protection (see fig. 6). Installing the latest security technology alone cannot guarantee effective facility protection if security personnel have not been adequately trained to use the technologies properly. Training is particularly essential if the technology requires personnel to master certain knowledge and skills to operate it, such as detecting concealed objects in generated X-ray images. Without adequate training in understanding how technology works, the security system will likely be less effective. This is especially important in assessing risks and vulnerabilities in facility protection. According to DHS officials, FPS inspectors are trained to conduct risk assessments and to evaluate the effectiveness of previously installed facility countermeasures. Trained FPS inspectors articulate their findings to a building security committee for approval and funding, after which FPS implements the necessary countermeasures. At the NAS symposium, a security consultant from the private sector said that the effectiveness of a risk management approach depends on the involvement of experienced and professional security personnel and that there is an increased chance that personnel could omit

[55]GAO, *Homeland Security: Transformation Strategy Needed to Address Challenges Facing the Federal Protective Service*, GAO-04-537 (Washington, D.C.: July 14, 2004).

[56]GAO-04-1033T.

[57]Department of Energy Inspector General, *Audit of the Department of Energy's Security Police Officer Training*, CR-B-95-03 (Washington, D.C.: Feb. 6, 1995).

major steps in the risk management process if they are not well trained in applying risk management.

Figure 6: FPS Officers Engaged in Biological and Chemical Weapons Response Training

Source: FPS.

As the emphasis on protecting people, property, and information has increased, it has made the demand for professional security practitioners

become even more important. It is widely recognized that there is a need for competent professionals who can effectively manage complex security programs that are designed to reduce threats to people and the assets of corporations, governments, and public and private institutions. To meet these needs, we noted an effort by one organization to provide standard certifications for security professionals. ASIS[58] International is an international organization for professionals responsible for security, including managers and directors of security. According to the ASIS International Web site, the organization is dedicated to increasing the effectiveness and productivity of security practices by developing educational programs and materials that address broad security concerns. ASIS International has put together a training curriculum where security professionals, upon completing requirements, can receive certifications to become Certified Protection Professionals, Professional Certified Investigators, or Physical Security Professionals (PSP). The PSP designation is the certification for those whose primary responsibility is to conduct threat surveys; design integrated security systems that include equipment, procedures and people; or install, operate and maintain those systems. We did not assess the training and certifications offered by ASIS International. Nonetheless, seeking certifications for security staff may allow agencies to better ensure that they are adequately trained and allows for comparisons with other organizations and the security industry.

Agencies Face Obstacles in Implementing Key Practices in Facility Protection

During our review, we noted that agencies face obstacles in implementing the six key practices that we have identified. For example, determining which assets to protect by establishing and sustaining a comprehensive risk management approach is a significant undertaking for federal agencies. The quality of information needed for the risk management process is often difficult to obtain and analyze. Another obstacle is keeping risk assessments up-to-date as threat levels change, and resources for this activity are stretched. As we pointed out earlier in relation to ISC's challenges, in our January 2003 high-risk report on federal real property, we highlighted that some major real property-holding agencies face obstacles in developing quality management data on their real property assets. Also, in April 2002, we reported that GSA's worldwide inventory of property contained data that were unreliable and of limited usefulness. This

[58] ASIS formerly stood for the American Society for Industrial Security; but now the organization refers to itself as ASIS International.

inventory is the only central source of descriptive data on the makeup of the federal real property inventory.[59]

In addition to data reliability problems, we have reported that some agencies face obstacles in implementing and leveraging security investments. As we testified in 2002, the capabilities of technology can be overestimated.[60] We found that by overestimating technology's capabilities, security officials risk falling into a false sense of security and relaxing their vigilance. Furthermore, technology cannot compensate for human failure. Instead, technology and people need to work together as part of an overall security process where security personnel are properly trained to use the technology.

The federal government also faces systemic obstacles regarding information sharing and coordination. We testified in August 2004 that there is a need for a comprehensive plan to facilitate information sharing and coordination in the protection of critical infrastructure.[61] However, DHS has not yet developed a plan that describes how it will carry out its overall information sharing responsibilities and relationships. In commenting on this report, DHS indicated in its technical comments that such an information plan is being developed. Another obstacle is developing productive information sharing relationships among federal, state, and local governments and the private sector. Improving the federal government's capabilities to analyze incident, threat, and vulnerability information from numerous sources could assist in more effectively disseminating information to federal, state, local, and private entities. Not sharing information on threats and on actual incidents experienced by others can hinder the ability of agencies' to identify new trends, better understand risks, and determine what preventive measures to implement. As we reported in August 2003, information sharing initiatives implemented by states and cities were neither effectively coordinated with those of federal agencies, nor were they coordinated within and between federal entities.[62]

[59]GAO, *Federal Real Property: Better Governmentwide Data Needed for Strategic Decisionmaking*, GAO-02-342 (Washington, D.C.: Apr. 16, 2002).

[60]GAO-02-687T.

[61]GAO-04-1033T.

[62]GAO-03-760.

At the agencywide level, we have reported that agencies face obstacles in developing meaningful, outcome-oriented performance goals and collecting performance data that can be used to assess the true impact of facility security. Performance measurement under GPRA typically focuses on regularly collected data on the level and type of program activities, the direct products and services delivered by the program, and the results of those activities. For programs that have readily observable results or outcomes, performance measurement may provide sufficient information to demonstrate program results. In some programs, such as facility security, however, outcomes are not quickly achieved or readily observed, or their relationship to the program is often not clearly defined. In such cases, more in-depth program evaluations may be needed, in addition to performance measurement, to examine the extent to which a program is achieving its objectives. This approach is more challenging and represents a more advanced level of performance measurement.

Significant long-standing obstacles also hinder agencies' ability to realign their asset portfolios. As we have reported, the complex legal and budgetary environment in which real property managers operate has a significant impact on real property decisionmaking and often does not lead to businesslike outcomes.[63] Resource limitations—including those related to facility protection—in general, often prevent agencies from addressing real property needs from a strategic portfolio perspective. When available funds for capital investment are limited, Congress must weigh the need for new, modern facilities with the need for renovation, maintenance, and disposal of existing facilities, the latter of which often gets deferred. Facility protection often falls within this latter category. Until these competing factors are mitigated, agencies face budgetary and legal disincentives when trying to realign their assets. State's experience to date with rightsizing its overseas presence demonstrated some of the challenges in realigning real property assets. We reported in November 2003 that State's efforts to replace facilities at risk of terrorist or other attacks have experienced project delays due to changes in project design and security requirements, difficulties hiring appropriate American and local labor with the necessary clearances and skills, differing site conditions, and unforeseen events such as civil unrest.[64]

[63]GAO-03-122.

[64]GAO, *Embassy Construction: State Department Has Implemented Management Reforms, but Challenges Remain*, GAO-04-100 (Washington, D.C.: Nov. 4, 2003).

Finally, we have reported that agencies continue to face obstacles in implementing and maintaining a strategic approach to human capital.[65] Specifically, agencies continue to face challenges in promoting (1) leadership; (2) strategic human capital planning; (3) acquiring, developing, and retaining talent; and (4) results-oriented organizational cultures in an effort to strategically manage human capital. Although some progress has been made since we designated human capital management as high-risk in 2001, today's federal human capital strategies are not appropriately constituted to meet current and emerging challenges, especially in light of the new security challenges facing the government. Human capital challenges are relevant to the facility protection area because security is a people-intensive activity involving active management and response, and there is a high dependency on law enforcement and security officers, as well as contract guards.

Given these obstacles, and the need to overcome them, agencies would benefit from having a set of key practices to guide their facility protection efforts. GAO has advocated the use of guiding principles in other areas, including human capital management, information technology, and capital investment.[66] ISC, in serving as the central coordinator for agencies' efforts, is uniquely positioned to promote key practices in facility protection and could use our work as a starting point. In fact, ISC views one of its primary roles as being the nucleus of communication on key practices and lessons learned for the facility protection community in the federal government and has embraced this responsibility.

Conclusions

After having limited success prior to the September 11 terrorist attacks, ISC has made progress in recent years related to its responsibilities to develop policies and standards, as well as those related to information sharing. Although this progress is encouraging, more work remains to fulfill ISC's major responsibilities related to ensuring agency compliance and overseeing the implementation of various policies and standards. Fulfilling its new role in reviewing and approving agencies' physical security plans for the administration represents a major step toward meeting its compliance and oversight responsibilities. Furthermore, because DHS now

[65]GAO, *High-Risk Series: Strategic Human Capital Management*, GAO-03-120 (Washington, D.C.: January 2003).

[66]See GAO-02-373SP; GAO/AIMD-99-32; GAO-04-791; and, GAO-04-546G.

has responsibility for ISC, the department also has a responsibility, in keeping with the executive order under which ISC was established, to ensure that ISC has adequate resources to accomplish its mission. Given the challenges ISC faces, its new responsibility related to HSPD-7 for reviewing agencies' physical security plans, and the need to sustain progress it has made in fulfilling its responsibilities, ISC would benefit from having a clearly defined action plan for achieving results. Such a plan, which ISC lacks, could be used to (1) provide DHS and other stakeholders with detailed information on, and a rationale for, its resource needs; (2) garner and maintain the support of ISC member agencies, DHS management, OMB, and Congress; (3) identify implementation goals and measures for gauging progress in fulfilling all of its responsibilities; and (4) propose strategies for addressing the challenges ISC faces. Such a plan could incorporate the strategy for ensuring compliance with facility protection standards that is required under ISC's executive order but has not yet been developed. Without an overall action plan for meeting this and other responsibilities, ISC's strategy and time line for these efforts remain unclear.

Since September 11, the focus on protecting the nation's critical infrastructure has been heightened considerably. At the individual building level, agencies have improved perimeter security by, for example, installing concrete bollards and are routinely screening vehicles and people entering federal property. In looking at facility protection issues more broadly, several key practices have emerged that include allocating resources using risk management, leveraging security technology, sharing information and coordinating protection efforts with other stakeholders, and measuring program performance and testing security initiatives. In addition, other key practices that have clear implications for the facility protection area include realigning real property assets and strategically managing human capital. Because agencies face various obstacles and would benefit from evaluating their actions, it would be useful for them to have a framework of key practices in the facility protection area that could guide their efforts, and ISC is well positioned to lead this initiative as the government's central forum for exchanging information and guidance on facility protection.

Recommendations for Executive Action

We are making two recommendations—one to the Secretary of Homeland Security and one to the Chair of ISC. Specifically, we recommend that the Secretary of Homeland Security direct the Chair of ISC to develop an action plan that identifies resource needs, implementation goals, and time frames for meeting ISC's ongoing and yet-unfulfilled responsibilities. The action

plan should also be used to propose strategies for addressing the range of challenges ISC faces. Such an action plan would provide a road map for DHS to use in developing resource priorities and for ISC to use in communicating its planned actions to agencies and other stakeholders, including Congress.

Furthermore, we recommend that the Chair of ISC, with input from ISC member agencies, consider using our work as a starting point for establishing a framework of key practices that could guide agencies' efforts in the facility protection area. This initiative could subsequently be used by agencies to evaluate their actions, identify lessons learned, and develop strategies for overcoming obstacles.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS, State, GSA, DOE, Interior, DOD, VA, and USPS for their official review and comment. DHS concurred with the report's overall conclusions and said it would implement the recommendations. In its comments, DHS provided information on ongoing initiatives related to information sharing and coordination. DHS's comments can be found in appendix V. DHS also provided separate technical comments, which we incorporated where appropriate. State provided additional information on its activities as they relate to the key practices, which we incorporated into the final report where appropriate. State's comments can be found in appendix VI. GSA, DOE, and Interior concurred with the report's findings and recommendations. Comments from GSA, Interior, and DOE can be found in appendixes VII, VIII, and IX, respectively. DOD, VA, and USPS notified us that they had no comments on this report.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to other interested Congressional Committees and the Secretaries of Defense, Energy, the Interior, Homeland Security, State, Veterans Affairs; the Administrator of GSA; and the Postmaster General of the U.S. Postal Service. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact me on (202) 512-2834 or at goldsteinm@gao.gov or David Sausville, Assistant Director, on (202) 512-5403 or at sausvilled@gao.gov. Other contributors to this report were Matt Cail, Roshni Dave, Joyce Evans, Brandon Haller, Anne Izod, Susan Michal-Smith, and Cynthia Taylor.

Sincerely yours,

Mark L. Goldstein
Director, Physical Infrastructure Issues

Objectives, Scope, and Methodology

Our objectives were to (1) assess the Interagency Security Committee's (ISC) progress in fulfilling its responsibilities and (2) identify key practices in protecting federal facilities and any related implementation obstacles. To assess ISC's progress in fulfilling its responsibilities, we interviewed the Executive Director of ISC; analyzed ISC publications and other documents; considered prior GAO work; and reviewed various laws and policies, including the Homeland Security Act of 2002. We also reviewed the executive order that established ISC, a subsequent executive order that amended it in connection with the transfer of ISC's function to DHS, and relevant homeland security policy directives. We also reviewed minutes from ISC meetings. We also considered prior GAO work on ISC. As part of our interviews with ISC's Executive Director, we focused on the challenges ISC faces in meeting its major responsibilities.

To identify key practices for facility protection and any related implementation obstacles, we conducted a comprehensive literature review of GAO and Inspector General (IG) reports, interviewed officials from the major property-holding agencies, and validated our results using an expert symposium on facility protection. For the analysis of GAO and IG reports, we systematically analyzed reports issued between January 1, 1995, and March 1, 2004. We chose 1995 as a starting point to coincide with the year of the terrorist attack on the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, and the publishing of the Justice Department's minimum-security standards.

We identified reports by searching GAO and IG online databases and consulting with GAO and IG contacts using several search terms such as facility security, terrorism, and homeland security. From this initial selection, we identified over 450 reports related to homeland security, which we subsequently reduced to 170 reports that were related to facility protection. Thirty-six of the reports were from IG offices at the seven agencies that control over 85 percent of federal facilities in terms of building square footage. These agencies included the Departments of Defense (DOD), Energy (DOE), the Interior (Interior), Veterans Affairs (VA) and State (State); the U.S. Postal Service (USPS); and the General Services Administration (GSA). We systematically reviewed these reports using a data collection instrument we designed to identify and group key practices according to theme or type of activity. In doing our work, we also gave consideration to other GAO reports on governmentwide management issues that, in our judgment, had implications for the facility protection area. We also considered new GAO reports that were issued after the selection time period that were relevant. For the purposes of this review,

we did not assess the extent to which agencies were using GPRA to develop agencywide facility protection or security-related goals. Also, for the purpose of this review, we did not assess the training and certifications offered by ASIS International.

We also interviewed officials at the major property-holding agencies, including DOD, DOE, Interior, VA, State, USPS, and GSA to obtain updated information on their facility protection activities and their use of key practices. We then contracted with the National Academy of Sciences (NAS) to convene a symposium with 21 security experts from the private sector, government, academia, and foreign countries to validate the practices and gain further insights. Using their judgment, NAS officials selected security experts based on their broad expertise and backgrounds in building security programs. Appendix II contains the symposium agenda and identifies the experts. As a result, for the purpose of this review, we defined key practices as those activities that, on the basis of our analysis, were recommended by GAO and others, acknowledged by agencies, and validated by experts in the area.

It is important to note that the key practices identified in this report may not be an exclusive list and may not necessarily represent all key practices for the protection of federal facilities. In addition, new reports and other information may have become available since we completed the analysis. Also, ISC has identified GAO as an associate member, which includes the ability to serve on ISC subcommittees. While associate members of ISC have this ability, no GAO staff member serves on any subcommittee. Furthermore, no GAO staff member actively participates in ISC meetings or contributes to decisions. Rather, GAO's role on ISC is only to observe proceedings and obtain ISC information distributed to the other ISC members. Because of GAO's observational role, our independence in making recommendations involving ISC and in completing this engagement was maintained.

ISC, agency officials, and other experts provided much of the data and other information used in this report. We noted cases where these officials provided testimonial evidence, and we were not always able to obtain documentation that would substantiate the testimonial evidence they provided. In cases where officials provided their views and opinions on various issues within the context of speaking for the organization, we corroborated the information with other officials. Overall, we found no discrepancies with these data and, therefore, determined that they were sufficiently reliable for the purpose of this report. We requested official

comments on this report from DHS, State, GSA, Interior, DOE, DOD, VA, and USPS. Appendixes V through IX contain comments we received from DHS, State, GSA, Interior, and DOE, respectively. We received State's comments on November 12, 2004. DOD, VA, and USPS had no comments.

National Academy of Sciences Symposium Agenda

Symposium on Security Efforts for Federal Real Property

March 4-5, 2004

National Academy of Sciences
Washington, D.C.
2101 C Street, NW, in Washington, D.C.
Thursday, March 4, 2004

Welcome and Introductory Remarks

Richard Little, Director, Board on Infrastructure and the Constructed Environment, National Research Council (NRC)
David Walker, Comptroller General, U.S. General Accounting Office

Keynote Address: The Modern Philosophy of Security

Roger Hagengruber, Director, Institute for Public Policy, University of New Mexico

Session 1

Wade Belcher, U.S. General Services Administration
Rick Jones, Naval Facilities Engineering Service Center
Curt Betts, Protective Design Center, U.S. Army Corps of Engineers
Wayne Ashbury, Bureau of Diplomatic Security

Session 2

Robert Smilowitz, Weidlinger and Associates
Kevin Claber, United Kingdom Government
Joe Smith, Applied Research Associates, Inc.
David Hadden, Ove Arup (United Kingdom)

Session 3

Doug Sunshine, Defense Threat Reduction Agency
John Crawford, Karagozian and Case
Randy Nason, C.H. Gurnsey
Eve Hinman, Hinman Consulting Engineers

Friday, March 5, 2004

Session 4

Elise Weaver, Worcester Polytechnic Institute
Robert Chapman, Building and Fire Research Laboratory, National Institute of Standards and Technology
Stuart Knoop, Oudens and Knoop
William Dowd, National Capital Planning Commission

Session 5

Johanna Hardy, Senate Government Affairs Committee
Susan Brita, House Transportation and Infrastructure Committee
Charles Herrick, Stratus Consulting
Paul Kleindorfer, The Wharton School
Michael O'Hanlon, The Brookings Institution

ISC Actions Related to Its Major Responsibilities under Executive Order 12977, as of September 2004

Responsibilities Related to Developing Policies and Standards
Establish policies for security in and protection of federal facilities. *Develop and evaluate security standards for federal facilities.* *Assess technology and information systems as a means of providing cost-effective improvements to security in federal facilities.* *Develop long-term construction standards for those locations with threat levels or missions that require blast-resistant structures or other specialized security requirements.* *Evaluate standards for the location of, and special security related to, day care centers in federal facilities.*
• May 2001: Issued Security Design Criteria for New Federal Office Buildings and Major Modernization Projects (Security Design Criteria). • July 2001: Issued Minimum Standards for Federal Building Access Procedures. • June 2003: Issued ISC Information Document on Escape Hoods. • October 2003: Issued update of ISC Security Design Criteria. • Currently developing physical security requirements for HSPD-12 and the federal credentialing program. • In 1997, ISC disseminated guidance on entry security technology for member agencies' buildings with high security designations. • Provided input in smart card development process for federal government. • Integrated expert opinions from engineering and architectural disciplines and included technology expert advice on blasting and biochemical threats in the most recent update of ISC Security Design Criteria for 2004. • July 2003: Issued Security Standards for Leased Space. • In its review of the latest ISC security design criteria update, the ISC long-term construction team will look into security needs at child care centers (no actions implemented to date).
Responsibilities Related to Ensuring Compliance and Overseeing Implementation of Policies and Standards
Develop a strategy for ensuring compliance with standards. *Oversee the implementation of appropriate security measures in federal facilities.*
• According to ISC's Executive Director, ISC does not have the necessary resources to develop a compliance process—ISC has requested additional funding and resources for the fiscal year 2006 budget (no actions implemented to date). • As reviewer of agency physical security plans under HSPD-7, ISC has not been able to develop a scoring process to review the plans. Furthermore, ISC will not meet the November 2004 deadline for completing agency reviews and is working with OMB and DHS on this issue.
Responsibilities Related to Encouraging Information Sharing
Encourage agencies with security responsibilities to share security-related intelligence in a timely and cooperative manner. *Assist in developing and maintaining a centralized security database of all federal facilities.*
• April 2003: Appointed a full-time Executive Director. • Since September 11, 2001, ISC has expanded its membership and outreach efforts by adding associate member agencies that can provide input but are not listed in Executive Order 12977. • September 2004: ISC issued Standard Operating Procedures. • ISC members meet regularly to facilitate an exchange of issues, concerns, and ideas between federal and private organizations. • Currently developing a secure Web portal system for member agencies to exchange information among authorized personnel. • Currently posts all finalized ISC standards, policies, guidance, and documents on GSA Office of Chief Architect's Web site for ISC members. • ISC does not have funding to support an initiative to develop a centralized security database and expects DHS to take the lead on this effort (no actions implemented to date).

Sources: GAO and DHS.

Risk Management Framework for Homeland Security and Terrorism

In recent years, GAO has consistently advocated the use of a risk management approach as an iterative analytical tool to help implement and assess responses to various national security and terrorism issues.[1] Although applying risk management principles to facility protection can take on various forms, our past work showed that most risk management approaches generally involve identifying potential threats, assessing vulnerabilities, identifying the assets that are most critical to protect in terms of mission and significance, and evaluating mitigation alternatives for their likely effect on risk and their cost. We have concluded that without a risk management approach, there is little assurance that programs to combat terrorism are prioritized and properly focused. Risk management principles acknowledge that while risk cannot be eliminated, enhancing protection from known or potential threats can help reduce it. Drawing on this precedent, we compiled a risk management framework—outlined below—to help assess the U.S. government's response to homeland security and terrorism risk. This framework, which we have used to assess the Department of Homeland Security's programs to target oceangoing cargo containers for inspection, also has applicability to protecting federal facilities. For purposes of the risk management framework, we used the following definitions:

- Risk—an event that has a potentially negative impact, and the possibility that such an event will occur and adversely affect an entity's assets and activities and operations, as well as the achievement of its mission and strategic objectives. As applied to the homeland security context, risk is most prominently manifested as "catastrophic" or "extreme" events related to terrorism, i.e., those involving more that $1 billion in damage or loss and/or more than 500 casualties.

- Risk management—a continuous process of managing, through a series of mitigating actions that permeate an entity's activities, the likelihood of an adverse event happening and having a negative impact. In general, risk is managed as a portfolio, addressing entity-wide risk within the entire scope of activities. Risk management addresses "inherent," or pre-action, risk (i.e., risk that would exist absent any mitigating action) as well as "residual," or post-action, risk (i.e., the risk that remains even after mitigating actions have been taken).

[1]See GAO-02-208T and GAO-02-150T.

The risk management framework—which is based on the proposition that a threat to a vulnerable asset results in risk—consists of the following components:

- Internal (or implementing) environment—the internal environment is the institutional "driver" of risk management, serving as the foundation of all elements of the risk management process. The internal environment includes an entity's organizational and management structure and processes that provide the framework to plan, execute, and control and monitor an entity's activities, including risk management. Within the organizational and management structure, an operational unit that is independent of all other operational (business) units is responsible for implementing the entity's risk management function. This unit is supported by and directly accountable to an entity's senior management. For its part, senior management (1) defines the entity's risk tolerance (i.e., how much risk is an entity willing to assume in order to accomplish its mission and related objectives) and (2) establishes the entity's risk management philosophy and culture (i.e., how an entity's values and attitudes view risk and how its activities and practices are managed to deal with risk). The operational unit (1) designs and implements the entity's risk management process and (2) coordinates internal and external evaluation of the process and helps implement any corrective action.

- Threat (event) assessment—threat is defined as a potential intent to cause harm or damage to an asset (e.g., natural environment, people, manmade infrastructures, and activities and operations). Threat assessments consist of the identification of adverse events that can affect an entity. Threats might be present at the global, national, or local level, and their sources include terrorists and criminal enterprises. Threat information emanates from "open" sources and intelligence (both strategic and tactical). Intelligence information is characterized as "reported" (or raw) and "finished" (fully fused and analyzed).

- Criticality assessment—criticality is defined as an asset's relative importance. Criticality assessments identify and evaluate an entity's assets based on a variety of factors, including the importance of its mission or function, the extent to which people are at risk, or the significance of a structure or system in terms of, for example, national security, economic activity, or public safety. Criticality assessments are important because they provide, in combination with the framework's

other assessments, the basis for prioritizing which assets require greater or special protection relative to finite resources.

- Vulnerability assessment—vulnerability is defined as the inherent state (either physical, technical, or operational) of an asset that can be exploited by an adversary to cause harm or damage. Vulnerability assessments identify these inherent states and the extent of their susceptibility to exploitation, relative to the existence of any countermeasures.

- Risk assessment—risk assessment is a qualitative and/or quantitative determination of the likelihood (probability) of occurrence of an adverse event and the severity, or impact, of its consequences. Risk assessments include scenarios under which two or more risks interact creating greater or lesser impacts.

- Risk characterization—risk characterization involves designating risk as, for example, low, medium, or high (other scales, such as numeric, are also be used). Risk characterization is a function of the probability of an adverse event occurring and the severity of its consequences. Risk characterization is the crucial link between assessments of risk and the implementation of mitigation actions, given that not all risks can be addressed because resources are inherently scarce; accordingly, risk characterization forms the basis for deciding which actions are best suited to mitigate the assessed risk.

- Mitigation evaluation—Mitigation evaluation is the identification of mitigation alternatives to assess the effectiveness of the alternatives. The alternatives should be evaluated for their likely effect on risk and their cost.

- Mitigation selection—Mitigation selection involves a management decision on which mitigation alternatives should be implemented among alternatives, taking into account risk, costs, and the effectiveness of mitigation alternatives. Selection among mitigation alternatives should be based upon preconsidered criteria. There are as of yet no clearly preferred selection criteria, although potential factors might include risk reduction, net benefits, equality of treatment, or other stated values. Mitigation selection does not necessarily involve prioritizing all resources to the highest-risk area, but in attempting to balance overall risk and available resources.

- Risk mitigation—Risk mitigation is the implementation of mitigation actions, in priority order and commensurate with assessed risk; depending on its risk tolerance, an entity may choose not to take any action to mitigate risk (this is characterized as risk acceptance). If the entity does choose to take action, such action falls into three categories: (1) risk avoidance (exiting activities that expose the entity to risk), (2) risk reduction (implementing actions that reduce likelihood or impact of risk), and (3) risk sharing (implementing actions that reduce likelihood or impact by transferring or sharing risk). In each category, the entity implements actions as part of an integrated "systems" approach, with built-in redundancy to help address residual risk (the risk that remains after actions have been implemented). The systems approach consists of taking actions in personnel (e.g., training, deployment), processes (e.g., operational procedures), technology (e.g., software or hardware), infrastructure (e.g., institutional or operational—such as port configurations), and governance (e.g., management and internal control and assurance). In selecting actions, the entity assesses their costs and benefits, where the amount of risk reduction is weighed against the cost involved and identifies potential financing options for the actions chosen.

- Monitoring and evaluation of risk mitigation—Monitoring and evaluation of risk mitigation entails the assessment of the functioning of actions against strategic objectives and performance measures to make necessary changes. Monitoring and evaluation includes, where and when appropriate, peer review and testing and validation; and an evaluation of the impact of the actions on future options; and identification of unintended consequences that, in turn, would need to be mitigated. Monitoring and evaluation helps ensure that the entire risk management process remains current and relevant, and reflects changes in (1) the effectiveness of the actions and (2) the risk environment in which the entity operates—risk is dynamic and threats are adaptive. The risk management process should be repeated periodically, restarting the "loop" of assessment, mitigation, and monitoring and evaluation.

Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

November 15, 2004

Mr. Mark L. Goldstein
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Goldstein:

RE: Draft Report GAO-05-49, Homeland Security: Further Actions Needed To Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices (GAO Job Code 543094)

Thank you for the opportunity to review and comment on the subject draft report. We appreciate the recognition of the significant progress the Interagency Security Committee (ISC) has achieved since moving to the Department of Homeland Security (DHS) in March 2003. The ISC, which is now chaired by DHS, is tasked with coordinating federal agencies' facility protection efforts, developing protection standards, and overseeing implementation. We view the recommendations as an opportunity to increase the effectiveness of ISC efforts in promoting a safe and secure environment for federal facilities, programs, employees and visitors.

We agree with the draft report's two recommendations and intend to implement them. GAO recommends the development of an action plan that identifies resource needs, implementation goals, and timeframes for meeting the ISC responsibilities. These responsibilities are stated in Executive Order 12977 as amended ("Interagency Security Committee") and Executive Order 13286 ("Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security"). GAO also recommends that the Chair of the ISC, with input from ISC member agencies, consider using GAO's work as a starting point for establishing a framework of key practices that could guide agencies' efforts in the facility protection area. Implementing this second recommendation should be beneficial in light of the new ISC responsibility under the Homeland Security Presidential Directive Number 7, Critical Infrastructure Identification, Prioritization and Protection to evaluate the effectiveness of all department and agency physical security plans.

We believe it is important that GAO recognize the existence of an ongoing program within the Department. In order to better assume the information sharing and coordination roles legislated to the Department of Homeland Security, Secretary Ridge charged the Under Secretary for Information Analysis and Infrastructure Protection (IAIP) to "develop a DHS-wide business plan for a comprehensive information sharing and collaboration system." Shortly thereafter, IAIP established an Information Sharing &

www.dhs.gov

Collaboration Program (ISCP) to discharge this responsibility. The ISCP is charged with the coordination and facilitation of information sharing efforts throughout the Department, and with its customers and partners in the federal, international, state, local, tribal and private sectors.

Numerous on-going information sharing initiatives within the homeland security, intelligence, law enforcement, and public safety communities must be leveraged by the ISCP to attain the program objectives. The role of the ISCP is to investigate, advise, recommend, and facilitate; other DHS components will be directly responsible for policy generation, technology and process development, and systems acquisition and implementation. These initiatives are crucial to producing comprehensive and practical approaches and solutions to address terrorist threats directed at federal facilities.

We have also provided you with technical comments under separate cover which we trust you will incorporate in the final report.

We thank you again for the opportunity to provide comments on this draft report and look forward to working with you on future homeland security issues.

Sincerely,

Anna F. Dixon
Director, Departmental GAO/OIG Liaison
Office of the Chief Financial Officer

MM/PGM

Comments from the Department of State

United States Department of State

Assistant Secretary and Chief Financial Officer

Washington, D.C. 20520

Ms. Jacquelyn Williams-Bridgers
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "HOMELAND SECURITY: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices," GAO Job Code 543094.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Cy Alba, Branch Chief, Bureau of Overseas Building Operations, at (703) 875-5748.

Sincerely,

Christopher B. Burnham

cc: GAO – Dave Sausville
OBO – Charles Williams
DS – Francis Taylor
State/OIG – Mark Duda

Department of State Comments on GAO Draft Report
"Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices"
(GAO-05-49, GAO Code 543094)

The Department of State (DOS) thanks the Government Accountability Office (GAO) for the opportunity to respond to their review of Federal Agencies Facility Protection Efforts. The draft report recommends that the Interagency Security Committee (ISC) establish a set of key practices to guide agencies' efforts in the facility protection area. Three key practices and the review summary are listed, followed by State's comments.

Now on p. 15.

Key Practice - Allocating Resources on the Basis of Risk Prioritizes Limited Security Resources (p. 17)

Homeland Security Presidential Directive Number-7 (HSPD-7) specifically directs DHS's Secretary to identify, **prioritize**, and protect critical infrastructure and key resources, so that these facilities can be protected from terrorist attack (pp. 7, 12). HSPD-7 establishes an **annual reporting cycle** for agencies to evaluate their critical infrastructure and key resources protection plans for both cyber and physical security (p. 12). [*emphasis added*] The Department of State suggests the following be added to GAO's list on pp. 19 and 20 of agency's examples of risk management to protect its facilities and how they were applied.

Now on pp. 17 and 18.

The Department of State's Long-Range Overseas Buildings Plan (LROBP) is a 6-year plan, updated yearly, that identifies embassy and consulate facilities most in need of replacement due to unacceptable security, safety, and/or operational condition. The plan identifies State's facilities program objectives and prioritizes competing facility requirements with input from the Bureaus of Overseas Buildings Operations (OBO) and Diplomatic Security (DS), State's Regional Bureaus, and other overseas agencies. The LROBP provides a roadmap for addressing long-term facility needs under the Capital Security Construction Program, Regular Capital Construction Program, as well as major rehabilitation, compound security, and other programs. To prepare the plan, each year OBO and DS meet with the Regional Bureaus to discuss which posts should move into the "top 80" list, which contains

the 80 primary posts requiring replacement for security reasons, and for which, by law, the Department can spend security capital construction appropriations. With respect to the original full list of facilities that need replacement, the Department, working with intelligence agencies, prioritizes these facilities.

Now on p. 29.

Key Practice – Performance Measurement Can Ensure Accountability for Achieving Broad Program Goals and Improved Security (p. 32)

The Department realizes that in this study, GAO did not assess the extent to which agencies were using GPRA to develop agency-wide facility protection or security-related goals (p. 34). GAO also notes (p. 32) that using performance measurement for facility protection is a practice that—based on its analysis—is in the early stages of development, although several initiatives used by other agencies were found.

State would like to note that in its annual Performance Assessment Rating Tool (PART) submission, that OBO's Capital Security Construction Program and DS's Worldwide Security Upgrades program are evaluated. State's PART submission can be viewed at www.whitehouse.gov/omb/part.

The OBO Capital Security Construction Program has been evaluated under PART over the past 3 years, and has recently received a 97% PART score. As of this date, no program in the Federal Government has received a PART score higher than 97%. Also, OBO's Regular/Asset Management Capital Construction Program was recognized as receiving one of the highest scores within the Department at its initial PART assessment with a score of 86%--an "effective" rating. The OBO compound security program has goals and performance measures also but has not been evaluated under PART; it will be this coming spring.

Key Practice – "Rightsizing" The Overseas Presence (p. 39)

Now on pp. 35-37.

The Department appreciates the discussion of rightsizing on pp. 39 and 40 of the draft report.

Now on p. 43.

Summary – Agencies Face Obstacles in Implementing Key Practices in Facility Protection (p. 46)

State would like to note that the challenges listed on pp. 48 and 49, such as difficulties hiring appropriate staff and differing site conditions, are not a function of rightsizing its overseas presence in and of itself, but rather a consequence of undertaking a large-scale program to construct new embassies in a foreign working environment in as short a time as possible. We would also like to note that the November 2003 GAO report[65] found that OBO began instituting management reforms for embassy building in 2001. The report also stated that while it is too early to assess the effectiveness of these reforms in ensuring that embassies are built within the approved project budget and on time, OBO now has a number of mechanisms in place to more effectively manage the expanded construction program.

[65]GAO, Embassy Construction: State Department Has Implemented Management Reform, but Challenges Remain, GAO-04-100 (Washington, D.C.: Nov. 4, 2003).

Comments from the General Services Administration

GSA U.S. General Services Administration

GSA PUBLIC BULDINGS SERVICE
Response to
Government Accountability Office

HOMELAND SECURITY: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices

November 12, 2004

GSA Public Buildings Service (PBS) Response

The PBS agrees with the findings of the Government Accountability Office (GAO) relating security issues facing the federal government. PBS also supports the recommendations to the Secretary of Department of Homeland Security and the Chair of Interagency Security Committee (ISC). As a member agency, of the ISC, GSA will support the initiatives and efforts proposed by the committee.

Summary of Audit Issues

✓ Reason GAO stated for conducting the subject audit:

1. Assess the Interagency Security Committee's (ISC) progress in fulfilling its responsibilities
2. Identify key practices in protecting federal facilities and any related implementation obstacles

✓ Audit Findings:

1. ISC made progress in government facility protection efforts
2. Action taken by ISC:
   - Develop policy and guidance
   - Sharing of information between agencies
3. July 2004, ISC became responsible for reviewing federal agencies physical security plans
4. ISC lacks an action plan for identifying implementation goals, strategy and timeline

✓ Summary

1. Audit Recommendations to the Secretary of DHS:
   - Direct ISC to develop an action plan that identifies resource needs, goals, and timeframes for meeting its responsibilities, and proposes strategies for addressing the challenges it faces.
2. Audit Recommendations to the Chair of ISC:
   - With input from ISC member agencies, and considering our work as a starting point, establish a set of key practices that could guide agencies' efforts in the facility protection

area. This effort could evaluate agency action, identify lessons learned, and develop strategies for overcoming challenges.

Comments from the Department of the Interior

United States Department of the Interior

OFFICE OF THE ASSISTANT SECRETARY
POLICY, MANAGEMENT AND BUDGET
Washington, D.C. 20240

NOV 10 2004

Mr. Mark L. Goldstein
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G. Street, NW, Mail Stop 2T23
Washington, D.C. 20548

Dear Mr. Goldstein:

Thank you for providing the Department of the Interior the opportunity to review and comment on the draft U.S. Government Accountability Office report entitled "Homelanc Security–Further Actions Needed To Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices," (GAO-05-49) dated November 2004.

We have reviewed the report and agree with the findings and recommendations.

Sincerely,

P. Lynn Scarlett
Assistant Secretary
Policy, Management and Budget

Comments from the Department of Energy

Department of Energy
Washington, DC 20585

November 10, 2004

Mr. Mark L. Goldstein
Director, Physical Infrastructure Issues
United States Government Accountability Office
441 G. Street, NW
Washington, DC 20548

Reference: Draft GAO Report 05-49, HOMELAND SECURITY - Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices

Dear Mr. Goldstein:

The Department of Energy, Office of Security, concurs with the discussion and recommendations contained in Draft GAO Report 05-49, HOMELAND SECURITY - Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices. We agree with the report's conclusions that closer coordination between agencies is an important element in improving the security and safety of all Federal worksites in a cost effective manner. We also agree that the Department of Homeland Security's Interagency Security Committee (ISC) is the appropriate entity to lead these coordination efforts. Furthermore, we believe that the actions recommended by the GAO will help to define a clear path forward for enhancing the security of all Government facilities, and we look forward to continuing to work with the ISC on this important National priority.

Thank you for the opportunity to review the draft report. If you wish to further discuss this matter, please do not hesitate to contact me at (202) 586-3345.

Sincerely,

Marshall O. Combs

Marshall O. Combs
Director, Office of Security
Office of Security and Safety
Performance Assurance

Printed with soy ink on recycled paper

Bibliography

Department of Defense

U.S. Department of Defense, Office of Inspector General. *Interagency Summary Report on Security Controls Over Biological Agents* (D-2003-126). Washington, D.C.: August 27, 2003.

Department of Energy

U.S. Department of Energy, Office of Inspector General. *Management of the Nuclear Weapons Production Infrastructure* (DOE/IG-0484). Washington, D.C.: September 22, 2000.

U.S. Department of Energy, Office of Inspector General. *Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process* (DOE/IG-0482). Washington, D.C.: September 28, 2000.

U.S. Department of Energy, Office of Inspector General. *The U.S. Department of Energy's Audit Follow-up Process* (DOE/IG-0447). Washington, D.C.: July 7, 1999.

U.S. Department of Energy, Office of Inspector General. *Special Audit Report on the Department of Energy's Arms and Military-Type Equipment* (IG-0385). Washington, D.C.: February 1, 1996.

U.S. Department of Energy, Office of Inspector General. *Audit of the Department of Energy's Security Police Officer Training* (CR-B-95-03). Washington, D.C.: February 6, 1995.

Department of the Interior

U.S. Department of the Interior, Office of Inspector General. *Homeland Security: Protection of Critical Infrastructure Systems – Assessment 2: Critical Infrastructure Systems* (2002-I-0053). Washington, D.C.: September 2002.

U.S. Department of the Interior, Office of Inspector General. *Homeland Security: Protection of Critical Infrastructure Facilities and National Icons – Assessment 1: Supplemental Funding – Plans and Progress* (2002-I-0039). Washington, D.C.: June 2002.

U.S. Department of the Interior, Office of Inspector General. *Progress Report: Secretary's Directives for Implementing Law Enforcement Reform in Department of the Interior* (2003-I-0062). Washington, D.C.: August 28, 2003.

U.S. Department of the Interior, Office of Inspector General. *Review of National Icon Park Security* (2003-I-0063). Washington, D.C.: August 2003.

Department of State

U.S. Department of State, Office of Inspector General. *Limited-Scope Security Inspection of Embassy Port of Spain, Trinidad and Tobago* (SIO-I-03-22). Washington, D.C.: August 2003.

U.S. Department of State, Office of Inspector General. *Security Inspection of Embassy N'Djamena, Chad* (SIO-I-03-27). Washington, D.C.: June 2003.

U.S. Department of State, Office of Inspector General. *Security Inspection of Embassy Yaoundé, Cameroon* (SIO-I-03-28). Washington, D.C.: March 2003.

U.S. Department of State, Office of Inspector General. *Security Inspection of Embassy Maseru, Lesotho* (SIO-I-03-26). Washington, D.C.: March 2003.

U.S. Department of State, Office of Inspector General. *Limited-Scope Security Inspection of Embassy Belgrade, Serbia and Montenegro* (SIO-I-03-13). Washington, D.C.: March 2003.

U.S. Department of State, Office of Inspector General. *Limited-Scope Security Inspection of Embassy Quito, Ecuador and Consulate General Guyaquil* (SIO-I-03-25). Washington, D.C.: February 2003.

U.S. Department of State, Office of Inspector General. *Security Oversight Inspection of Embassy Muscat, Oman* (SIO-I-03-17). Washington, D.C.: February 2003.

U.S. Department of State, Office of Inspector General. *Limited-Scope Security Inspection of Embassy Dublin, Ireland* (SIO-I-03-08). Washington, D.C.: December 2002.

U.S. Department of State, Office of Inspector General. *Limited-Scope Security Inspection of Embassy Apia, Samoa* (SIO-I-03-04). Washington, D.C.: November 2002.

U.S. Department of State, Office of Inspector General. *Limited-Scope Security Inspection of Embassy Ljubljana, Slovenia* (SIO-I-03-03). Washington, D.C.: November 2002.

U.S. Department of State, Office of Inspector General. *Limited-Scope Security Inspection of Embassy Almaty, Kazakhstan* (SIO-I-03-02). Washington, D.C.: November 2002.

U.S. Department of State, Office of Inspector General. *Limited-Scope Security Inspection of Embassy Amman, Jordan* (SIO-I-03-01). Washington, D.C.: November 2002.

U.S. Department of State, Office of Inspector General. *Classified Semiannual Report to the Congress: April 1, 2003 to September 30, 2003.* Washington, D.C.: September 2003.

U.S. Department of State, Office of Inspector General. *Classified Semiannual Report to the Congress: October 1, 2002 to March 31, 2003.* Washington, D.C.: March 2003.

General Services Administration

General Services Administration, Office of Inspector General. *Follow-up Review of the Federal Protective Service's Contract Guard Program* (A020092/P/2/R02016). Arlington, VA: August 29, 2002.

General Services Administration, Office of Inspector General. *Report on Federal Protective Service Security Equipment Countermeasures Installed at Federal Facilities* (A020092/P/2/R02008). Arlington, VA: March 29, 2002.

General Services Administration, Office of Inspector General. *Audit of the Federal Protective Service's Federal Security Risk Manager Program* (A010129/P/2/R02007). Arlington, VA: March 27, 2002.

General Services Administration, Office of Inspector General. *Audit of the Federal Protective Service's Intelligence Sharing Program* (A000992/P/2/R01013). Arlington, VA: March 23, 2001.

General Services Administration, Office of Inspector General. *Audit of The Federal Protective Service's Contract Guard Program* (A995175/P/2/R00010). Arlington, VA: March 28, 2000.

General Services Administration, Office of Inspector General. *Audit of Security Measures for New and Renovated Federal Facilities* (A995025/P/H/R99513). Arlington, VA: March 24, 1999.

General Services Administration, Office of Inspector General. *Audit of The Federal Protective Service's Program for Upgrading Security at Federal Facilities* (A70642/P/2/R98024). Arlington, VA: September 14, 1998.

Postal Service

U.S. Postal Service, Office of Inspector General. *Fiscal Year 1999 Information System Controls: St. Louis Information Service Center* (FR-AR-99-010). Arlington, VA: September 28, 1999.

U.S. Postal Service, Office of Inspector General. *Review of Security Badge Controls at Postal Service Headquarters* (OV-LA-01-001). Arlington, VA: March 26, 2001.

U.S. Postal Service, Office of Inspector General. *Review of United States Postal Service Personnel Security Program: Process for Updating Sensitive Clearances* (OV-MA-99-001). Arlington, VA: March 31, 1998.

Veterans Affairs

Veterans Affairs, Office of Inspector General. *Review of Security and Inventory Controls Over Selected Biological, Chemical, and Radioactive Agents Owned by or Controlled at Department of Veterans Affairs Facilities* (02-00266-76). Washington, D.C.: March 14, 2002.

Related GAO Products

Allocating Resources Using Risk Management

Fiscal Year 2003 U.S. Government Financial Statements: Sustained Improvement in Federal Financial Management Is Crucial to Addressing Our Nation's Future Fiscal Challenges. GAO-04-886T. Washington, D.C.: July 8, 2004.

Nuclear Security: Several Issues Could Impede the Ability of DOE's Office of Energy, Science and Environment to Meet the May 2003 Design Basis Threat. GAO-04-894T. Washington, D.C.: June 22, 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. GAO-04-557T. Washington, D.C.: March 31, 2004.

Homeland Security: Management Challenges Facing Federal Leadership. GAO-03-260. Washington, D.C.: December 20, 2002.

Critical Infrastructure Protection: Significant Challenges Need to Be Addressed. GAO-02-961T. Washington, D.C.: July 24, 2002.

Homeland Security: Critical Design and Implementation Issues. GAO-02-957T. Washington, D.C.: July 17, 2002.

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. GAO-02-918T. Washington, D.C.: July 9, 2002.

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts. GAO-02-208T. Washington, D.C.: October 31, 2001.

Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness. GAO-02-162T. Washington, D.C.: October 17, 2001.

Homeland Security: Key Elements of a Risk Management Approach. GAO-02-150T. Washington, D.C.: October 12, 2001.

Chemical and Biological Defense: Improved Risk Assessment and Inventory Management Are Needed. GAO-01-667. Washington, D.C.: September 28, 2001.

Combating Terrorism: Selected Challenges and Related Recommendations. GAO-01-822. Washington, D.C.: September 20, 2001.

Combating Terrorism: Actions Needed to Improve DOD Antiterrorism Program Implementation and Management. GAO-01-909. Washington, D.C.: September 19, 2001.

Weapons of Mass Destruction: Defense Threat Reduction Agency Addresses Broad Range of Threats, but Performance Reporting Can Be Improved. GAO-04-330. Washington, D.C.: February 13, 2004.

Leveraging Technology

Electronic Government: Smart Card Usage is Advancing Among Federal Agencies, Including the Department of Veterans Affairs. GAO-05-84T. Washington, D.C: September 6, 2004.

Information Security: Technologies to Secure Federal Systems. GAO-04-467. Washington, D.C.: March 9, 2004.

Security: Counterfeit Identification Raises Homeland Security Concerns. GAO-04-133T. Washington, D.C.: October 1, 2003.

Electronic Government: Challenges to the Adoption of Smart Card Technology. GAO-03-1108T. Washington, D.C.: September 9, 2003.

Information Security: Challenges in Using Biometrics. GAO-03-1137T. Washington, D.C.: September 9, 2003.

Border Security: Challenges in Implementing Border Technology. GAO-03-546T. Washington, D.C.: March 12, 2003.

Electronic Government: Progress in Promoting Adoption of Smart Card Technology. GAO-03-144. Washington, D.C.: January 3, 2003.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. Washington, D.C.: November 15, 2002.

National Preparedness: Technologies to Secure Federal Buildings. GAO-02-687T. Washington, D.C.: April 25, 2002.

Information Sharing and Coordination

Information Technology: Major Federal Networks That Support Homeland Security Functions. GAO-04-375. Washington, D.C.: September 17, 2004

9/11 Commission Report: Reorganization, Transformation, and Information Sharing. GAO-04-1033T. Washington, D.C.: August 3, 2004.

Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors. GAO-04-780. Washington, D.C.: July 9, 2004.

Posthearing Questions from September 17, 2003, Hearing on "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electrical Grid, Critical Interdependencies, Vulnerabilities, and Readiness". GAO-04-300R. Washington, D.C.: December 8, 2003.

Homeland Security: Challenges in Achieving Interoperable Communications for First Responders. GAO-04-231T. Washington, D.C.: November 6, 2003.

Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues. GAO-03-1165T. Washington, D.C.: September 17, 2003.

Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened. GAO-03-760. Washington, D.C.: August 27, 2003.

Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues. GAO-03-715T. Washington, D.C.: May 8, 2003.

Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integrating and Sharing. GAO-03-322. Washington, D.C.: April 15, 2003.

Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies. GAO-03-139. Washington, D.C.: May 30, 2003.

Homeland Security: Information Sharing Activities Face Continued Management Challenges. GAO-02-1122T. Washington, D.C.: October 1, 2002.

National Preparedness: Technology and Information Sharing Challenges. GAO-02-1048R. Washington, D.C.: August 30, 2002.

Homeland Security: Effective Intergovernmental Coordination is Key to Success. GAO-02-1013T. Washington, D.C.: August 23, 2002.

Homeland Security: Effective Intergovernmental Coordination is Key to Success. GAO-02-1012T. Washington, D.C.: August 22, 2002.

Homeland Security: Effective Intergovernmental Coordination is Key to Success. GAO-02-1011T. Washington, D.C.: August 20, 2002.

Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success. GAO-02-901T. Washington, D.C.: July 3, 2002.

Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success. GAO-02-900T. Washington, D.C.: July 2, 2002.

Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success. GAO-02-899T. Washington, D.C.: July 1, 2002.

National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts is Critical to an Effective National Strategy for Homeland Security. GAO-02-621T. Washington, D.C.: April 11, 2002.

Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness. GAO-02-550T. Washington, D.C.: April 2, 2002.

Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy. GAO-02-549T. Washington, D.C.: March 28, 2002.

Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness. GAO-02-548T. Washington, D.C.: March 25, 2002.

Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness. GAO-02-547T. Washington, D.C.: March 22, 2002.

Homeland Security: Progress Made; More Direction and Partnership Sought. GAO-02-490T. Washington, D.C.: March 12, 2002.

Combating Terrorism: Key Aspects of a National Strategy to Enhance State and Local Preparedness. GAO-02-473T. Washington, D.C.: March 1, 2002.

Bioterrorism: Review of Public Health Preparedness Programs. GAO-02-149T. Washington, D.C.: October 10, 2001.

Bioterrorism: Public Health and Medical Preparedness. GAO-02-141T. Washington, D.C.: October 9, 2001.

Bioterrorism: Coordination and Preparedness. GAO-02-129T. Washington, D.C.: October 5, 2001.

Combating Terrorism: Observations on Federal Spending to Combat Terrorism. GAO/T-NSIAD/GGD-99-107. Washington, D.C.: March 11, 1999.

Aligning Assets to Mission

Embassy Construction: State Department Has Implemented Management Reforms, but Challenges Remain. GAO-04-100. Washington, D.C.: November 4, 2003.

VA Health Care: Framework for Analyzing Capital Asset Realignment for Enhanced Services Decisions. GAO-03-1103R. Washington, D.C.: August 18, 2003.

Major Management Challenges and Program Risks: Department of State. GAO-03-107. Washington, D.C.: January 2003.

Overseas Presence: Framework for Assessing Embassy Staff Levels Can Support Rightsizing Initiatives. GAO-02-780. Washington, D.C.: July 26, 2002.

Overseas Presence: Observations on a Rightsizing Framework. GAO-02-659T. Washington, D.C.: May 1, 2002.

Overseas Presence: More Work Needed on Embassy Rightsizing. GAO-02-143. Washington, D.C.: November 27, 2001.

Strategic Human Capital Management

Human Capital: Building on the Current Momentum to Transform the Federal Government. GAO-04-976T. Washington, D.C.: July 20, 2004.

Information Technology: Training Can Be Enhanced by Greater Use of Leading Practices. GAO-04-791. Washington, D.C.: June 24, 2004.

Results-Oriented Government: Shaping the Government to Meet 21st Century Challenges. GAO-03-1168T. Washington, D.C.: September 17, 2003.

Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success. GAO-03-488. Washington, D.C.: March 14, 2003.

Human Capital: Building on the Current Momentum to Address High-Risk Issues. GAO-03-637T. Washington, D.C.: April 8, 2003.

High-Risk Series: Strategic Human Capital Management. GAO-03-120. Washington, D.C.: January 2003.

Human Capital: A Self-Assessment Checklist for Agency Leaders. GAO/OCG-00-14G. Washington, D.C.: September 2000.

Executive Guide: Leading Practices in Capital Decision-Making. AIMD-99-32. Washington, D.C.: December 1998.

Performance Measurement and Testing

Weaknesses in Screening Entrants Into the United States. GAO-03-438T. Washington, D.C.: January 30, 2003.

Building Security: Interagency Security Committee Has Had Limited Success in Fulfilling Its Responsibilities. GAO-02-1004. Washington, D.C.: September 17, 2002.

Security Breaches at Federal Buildings in Atlanta, Georgia. GAO-02-668T. Washington, D.C.: April 30, 2002.

Homeland Security: Responsibility and Accountability For Achieving National Goals. GAO-02-627T. Washington, D.C.: April 11, 2002.

Bioterrorism: Federal Research and Preparedness Activities. GAO-01-915. Washington, D.C.: September 28, 2001.

Combating Terrorism: Observations on Options to Improve the Federal Response. GAO-01-660T. Washington, D.C.: April 24, 2001.

Combating Terrorism: Analysis of Federal Counterterrorist Exercises. GAO/NSIAD-99-157BR. Washington, D.C.: June 25, 1999.

Federal Law Enforcement: Investigative Authority and Personnel at 13 Agencies. GAO/GGD-96-154. Washington, D.C.: September 30, 1996.

Challenges and Lessons Learned in Homeland Security

Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. GAO-03-233. Washington, D.C.: February 28, 2003.

Combating Terrorism: Funding Data Reported to Congress Should Be Improved. GAO-03-170. Washington, D.C.: November 26, 2002.

Combating Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations. GAO-03-14. Washington, D.C.: November 1, 2002.

Homeland Security: Challenges and Strategies in Addressing Short-and Long-Term National Needs. GAO-02-160T. Washington, D.C.: November 7, 2001.

Combating Terrorism: FEMA Continues to Make Progress in Coordinating Preparedness and Response. GAO-01-15. Washington, D.C.: March 20, 2001.

Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination. GAO/T-AIMD-00-268. Washington, D.C.: July 26, 2000.

Combating Terrorism: Observations on Growth in Federal Programs. GAO/T-NSIAD-99-181. Washington, D.C.: June 9, 1999.

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination. GAO/NSIAD-98-39. Washington, D.C.: December 1, 1997.

Other Products Related to Facility Security

Homeland Security: Transformation Strategy Needed to Address Challenges Facing the Federal Protective Service. GAO-04-537. Washington, D.C.: July 14, 2004.

General Services Administration: Factors Affecting the Construction and Operating Costs of Federal Buildings. GAO-03-609T. Washington, D.C.: April 2, 2003.

High-Risk Series: Federal Real Property. GAO-03-122. Washington, D.C.: January 2003.

Building Security: Security Responsibilities for Federally Owned and Leased Facilities. GAO-03-8. Washington, D.C.: October 31, 2002.

Diffuse Security Threats: USPS Air Filtration Systems Need More Testing and Cost Benefit Analysis before Implementation. GAO-02-838. Washington, D.C.: August 22, 2002.

Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains. GAO-02-610. Washington, D.C.: June 7, 2002.

Federal Real Property: Better Governmentwide Data Needed for Strategic Decisionmaking. GAO-02-342. Washington, D.C.: April 16, 2002.

Highlights of GAO's Conference on Options to Enhance Mail Security and Postal Operations. GAO-02-315SP. Washington, D.C.: December 20, 2001.

General Services Administration: Status of Efforts to Improve Management of Building Security Upgrade Program. GAO/T-GGD/OSI-00-19. Washington, D.C.: October 7, 1999

General Services Administration: Many Building Security Upgrades Made But Problems Have Hindered Program Implementation. GAO/T-GGD-98-141. Washington, D.C.: June 4, 1998.

Other Products Related to Security Topics

Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism. GAO-04-408T. Washington, D.C.: February 3, 2004.

Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange. GAO-04-453R. Washington, D.C.: February 26, 2004.

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. GAO-04-325T. Washington, D.C.: December 16, 2003.

Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs. GAO-04-285T. Washington, D.C.: November 20, 2003.

Bioterrorism: A Threat to Agriculture and the Food Supply. GAO-04-259T. Washington, D.C.: November 19, 2003.

Aviation Security: Efforts to Measure Effectiveness and Address Challenges. GAO-04-232T. Washington, D.C.: November 5, 2003.

Aviation Security: Progress Since September 11, 2001 and the Challenges Ahead. GAO-03-1150T. Washington, D.C.: September 9, 2003.

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO-03-616T. Washington, D.C.: April 1, 2003.

Combating Terrorism: Observations on National Strategies Related to Terrorism. GAO-03-519T. Washington, D.C.: March 3, 2003.

Overseas Presence: Conditions of Overseas Diplomatic Facilities. GAO-03-557T. Washington, D.C.: March 20, 2003.

Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges. GAO-03-263. Washington, D.C.: December 13, 2002.

Mass Transit: Challenges in Securing Transit Systems. GAO-02-1075T. Washington, D.C.: September 18, 2002.

Combating Terrorism: Department of State Programs to Combat Terrorism Abroad. GAO-02-1021. Washington, D.C.: September 6, 2002.

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T. Washington, D.C.: August 5, 2002.

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy. GAO-02-811T. Washington, D.C.: June 7, 2002.

Homeland Security: A Framework for Addressing the Nation's Efforts. GAO-01-1158T. Washington, D.C.: September 21, 2001.

Combating Terrorism: Comments on H.R. 525 to Create a President's Council on Domestic Terrorism Preparedness. GAO-01-555T. Washington, D.C.: May 9, 2001.

Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy. GAO-01-556T. Washington, D.C.: March 27, 2001.

Embassy Construction: Better Long-Term Planning Will Enhance Program Decision-making. GAO-01-11. Washington, D.C.: January 22, 2001.

FAA Computer Security: Recommendations to Address Continuing Weaknesses. GAO-01-171. Washington, D.C.: December 6, 2000.

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations. GAO/T-AIMD-00-330. Washington, D.C.: September 27, 2000.

FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses. GAO/AIMD-00-252. Washington, D.C.: August 16, 2000.

Combating Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas. GAO/NSIAD-00-181. Washington, D.C.: July 19, 2000.

State Department: Overseas Emergency Security Program Progressing, but Costs Are Increasing. GAO/NSIAD-00-83. Washington, D.C.: March 8, 2000.

Combating Terrorism: Issues in Managing Counterterrorist Programs. GAO/T-NSIAD-00-145. Washington, D.C.: April 6, 2000.

State Department: Progress and Challenges in Addressing Management Issues. GAO/T-NSIAD-00-124. Washington, D.C.: March 8, 2000.

State Department: Major Management Challenges and Program Risks. GAO/T-NSIAD/AIMD-99-99. Washington, D.C.: March 4, 1999.

Major Management Challenges and Program Risks: Department of State. GAO/OCG-99-12. Washington, D.C.: January 1999.

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency. GAO/NSIAD-99-3. Washington, D.C.: November 12, 1998.

Foreign Affairs Management: Major Challenges Facing the Department of State. GAO/T-NSIAD-98-251. Washington, D.C.: September 17, 1998.

Combating Terrorism: Efforts to Protect U.S. Forces in Turkey and the Middle East. GAO/T-NSIAD-98-44. Washington, D.C.: October 28, 1997.

Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy. GAO/NSIAD-97-254. Washington, D.C.: September 26, 1997.

Combating Terrorism: Status of DOD Efforts to Protect Its Forces Overseas. GAO/NSIAD-97-207. Washington, D.C.: July 21, 1997.

Aviation Security: FAA's Procurement of Explosives Detection Devices. GAO/RCED-97-111R. Washington, D.C.: May 1, 1997.

Aviation Security: Posting Notices at Domestic Airports. GAO/RCED-97-88R. Washington, D.C.: March 25, 1997.

Aviation Security: Technology's Role in Addressing Vulnerabilities. GAO/T-RCED/NSIAD-96-262. Washington, D.C.: September 19, 1996.

Aviation Security: Urgent Issues Need to Be Addressed. GAO/T-RCED/NSIAD-96-251. Washington, D.C.: September 11, 1996.

Aviation Security: Immediate Action Needed to Improve Security. GAO/T-RCED/NSIAD-96-237. Washington, D.C.: August 1, 1996.

Aviation Security: FAA Can Help Ensure That Airports' Access Control Systems are Cost-Effective. GAO/RCED-95-25. Washington, D.C.: March 1, 1995.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Susan Becker, Acting Manager, BeckerS@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548