

GAO

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

May 2006

HOMELAND SECURITY

Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-06-612](#), a report to the Chairman, Committee on Government Reform, House of Representatives

Why GAO Did This Study

The protection of U.S. federal facilities has become an important concern due to the ongoing threat of terrorism. The General Services Administration (GSA), U.S. Postal Service (USPS), and the Departments of Veterans Affairs (VA) and Interior (Interior) hold the most domestic, nonmilitary property. Additionally, the Department of Homeland Security (DHS) is responsible for the protection of GSA facilities. DHS chairs the Interagency Security Committee (ISC), which is tasked with coordinating federal agencies' facility protection efforts. The need to better protect federal facilities, as well as federal budget constraints, have prompted the need for these agencies to measure the performance of their facility protection efforts. GAO's objectives were (1) to identify examples of performance measures for facility protection being used by selected organizations outside of the federal government; and (2) to determine the status of U.S. federal agencies' efforts to develop and use performance measures as a part of their facility protection programs.

What GAO Recommends

GAO is recommending that the Secretary of DHS direct ISC to establish guidance and standards for measuring performance in federal government facility protection. DHS agreed with the findings and recommendations in this report.

www.gao.gov/cgi-bin/getrpt?GAO-06-612.

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

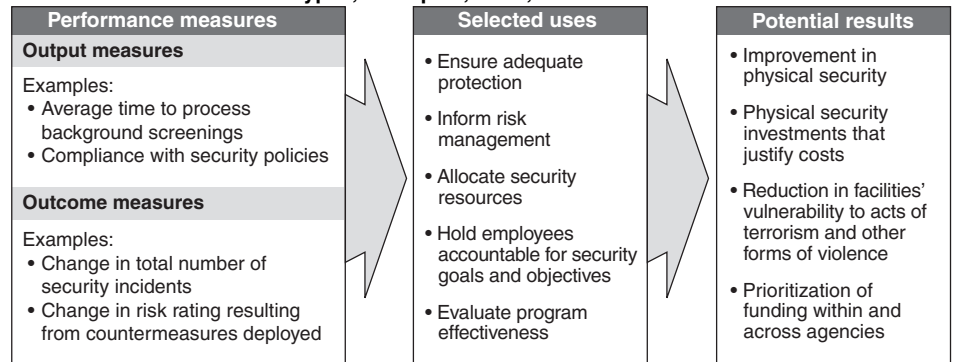
HOMELAND SECURITY

Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts

What GAO Found

GAO found a range of examples of performance measures that organizations outside the U.S. government—including private-sector entities, state and local governments, and foreign government agencies—have developed that, collectively, indicate whether facility protection efforts are achieving results (see figure below). These organizations use security-related performance measures to help improve security, make decisions about risk management and resource allocation, and hold employees accountable for whether a program meets its security goals and objectives. However, many of the organizations said that developing and using these measures can be challenging and that they look to the U.S. government for assistance and leadership in developing standards and guidance for facility protection.

Performance Measurement Types, Examples, Uses, and Results



Source: GAO

Note: Output measures focus on the direct product/services delivered by a program. Outcome measures provide information on the results of products/services.

We found that some bureaus and services within DHS (for GSA properties), USPS, and Interior are using security performance measures, while VA and other bureaus and services within the three agencies collect data that could be used to measure security performance. Agencies that have performance measures use them to ensure adequate protection at individual facilities, make risk management decisions, and evaluate program effectiveness. However, agencies face challenges—similar to those cited by nonfederal entities—in further developing and using security performance measures. Currently, there is no governmentwide guidance or standards on measuring facility protection performance to help federal agencies address these challenges. This differs from information technology security, where agencies have detailed, governmentwide guidance for developing and using performance measures. Without effective performance measurement data, decision makers may have insufficient information to evaluate whether their investments have improved security or reduced federal facilities' vulnerability to acts of terrorism or other forms of violence. ISC is uniquely positioned to develop and disseminate guidance and standards for measuring the performance of federal government facility protection efforts.

Contents

Letter		1
	Results in Brief	4
	Background	6
	Organizations outside of the U.S. Government Use Security Performance Measures to Enhance Decision Making and Help Ensure Accountability	12
	U.S. Agencies Have Made Some Progress in Developing and Using Performance Measures for Facility Protection Programs, but Lack Guidance and Standards	25
	Conclusions	48
	Recommendations for Executive Action	49
	Agency Comments and Our Evaluation	49
Appendix I	Objectives, Scope, and Methodology	52
Appendix II	Examples of Performance Measures Used by Selected Organizations outside of the Federal Government	58
Appendix III	Comments from the Department of Homeland Security	62
Appendix IV	Comments from the Department of the Interior	64
	GAO Comments	67
Appendix V	GAO Contact and Staff Acknowledgments	68
Tables		
	Table 1: Examples of Performance Measures for Facility Protection	13
	Table 2: FPS’s Performance Measures for Facility Protection	26
	Table 3: BOR’s Performance Measures for Facility Protection	32
	Table 4: Inspection Service’s Performance Measure for Facility Protection	34

Table 5: Types of Information Technology Security Performance Measures Described by NIST	41
Table 6: U.S. State and Local Governments Contacted	54
Table 7: Foreign Government Agencies and Organizations Visited	55

Figures

Figure 1: Smart Card Access Portals at a Federal Building Entrance	9
Figure 2: Linkages between District of Columbia Strategic Goals and Performance Measures for Facility Protection	20
Figure 3: Linkages between DHS Mission and FPS Performance Measures for Facility Protection	29
Figure 4: Linkages between USPS Inspection Service Strategic Goals and Performance Measure for Facility Protection	37
Figure 5: Sample Standardized Performance Measurement Data Form	44

Abbreviations

BOR	Bureau of Reclamation
DHS	Department of Homeland Security
DSO	departmental security officer
FPS	Federal Protective Service
GPRA	Government Performance and Results Act of 1993
GSA	General Services Administration
HSPD-7	Homeland Security Presidential Directive Number 7
ICE	Immigration and Customs Enforcement
ISC	Interagency Security Committee
IT	information technology
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NM&I	National Monuments and Icons Assessment Methodology
OLES	Office of Law Enforcement and Security
OMB	Office of Management and Budget
PART	Program Assessment Rating Tool
USPS	United States Postal Service
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

May 31, 2006

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

Dear Mr. Chairman:

The threat of terrorism has increased the emphasis on physical security for federal real property assets since the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City; the 1998 embassy bombings in Africa; the September 11, 2001, attacks on the World Trade Center and the Pentagon; and the anthrax attacks in the fall of 2001. The federal government owns or leases an estimated 3.2 billion square feet of space within the United States in more than 450,000 buildings, which are regularly accessed by millions of federal employees, contractors, and citizens. Approximately 42 percent of this square footage is nonmilitary property, and a majority of this is under the control or custody of the General Services Administration (GSA), the United States Postal Service (USPS), the Department of Veterans Affairs (VA), and the Department of the Interior (Interior).¹ Under the Homeland Security Act of 2002, the Federal Protective Service (FPS), which protects GSA properties, was transferred to the Department of Homeland Security (DHS). For agencies that aim to ensure public access to their assets, protecting nonmilitary real property assets can be complex and contentious because of the need to strike a balance between public access and security.² Federal agencies face additional security-related challenges, such as securing federally leased space and addressing conflicts with state, local, or private entities that also have jurisdiction over, or input regarding, physical security enhancements. The challenge of protecting federal facilities against the

¹GSA, *Overview of the United States Government's Owned and Leased Real Property: Federal Real Property Profile As of September 30, 2004* (Washington, D.C.). This property includes government-owned and leased space.

²GAO, *Homeland Security: Actions Needed to Better Protect National Icons and Federal Office Buildings from Terrorism*, [GAO-05-790](#) (Washington, D.C.: June 24, 2005), p. 1.

threat of terrorism was a major reason GAO designated federal real property as a high-risk area in January 2003.³

Although FPS is primarily responsible for protecting GSA properties, it also has responsibility for broader efforts across the federal government to enhance the protection of critical facilities and works closely with the Interagency Security Committee (ISC) on these issues. The ISC, which DHS chairs, is tasked with coordinating federal agencies' facility protection efforts, developing protection standards, and overseeing implementation of those standards.⁴ In November 2004, we recommended that ISC develop an action plan for fulfilling its responsibilities and establish a set of key practices for facility protection.⁵ We identified several key practices in facility protection, which included using risk management to allocate resources;⁶ leveraging security technology; coordinating protection efforts and sharing information; realigning real property assets to an agency's mission, thereby reducing vulnerabilities; strategically managing human capital; and measuring program

³GAO, *High-Risk Series: Federal Real Property*, [GAO-03-122](#) (Washington, D.C.: January 2003).

⁴In this report, facility protection denotes the protection of not only the facilities but also the people, equipment, and other assets within them. Additionally, this report focuses largely on protecting facilities from threats and acts of terrorism. However, it is important to note that facilities are also vulnerable to other types of hazards, such as natural disasters and workplace violence, and information in this report may be applicable to those hazards as well.

⁵GAO, *Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices*, [GAO-05-49](#) (Washington, D.C.: Nov. 30, 2004). Since the time of that report, the ISC Chair noted that he is in the process of creating and establishing an action plan with the ISC membership, although little progress has been made because of limited resources. The Chair anticipates that this action plan, which will articulate a roadmap for the ISC to follow in meeting its responsibilities, will incorporate portions of the material and related concepts contained in GAO reports.

⁶Risk management is a tool for assessing risks, evaluating alternatives, making decisions, and implementing and monitoring protective measures. More specifically, risk can be calculated as follows: risk = (threat x vulnerability) x consequence. *Threat* is the probability that a specific type of attack will be initiated against a particular target or class of targets. The *vulnerability* of an asset is the probability that a particular attempted attack will succeed against a particular target or class of targets. It is usually measured against some set of standards, such as availability/predictability, accessibility, countermeasures in place, and target hardness (the material construction characteristics of the asset). The *consequence* of a terrorist attack is characterized as the expected worst case or worst reasonable adverse impact of a successful attack.

performance and testing security initiatives.⁷ With regard to measuring performance, performance measures can be classified as output measures, which focus on the quantity of direct products and services a program delivers; outcome measures, which offer information on the results of the direct products and services a program has delivered; or process/input measures, which address the type or level of program activity an organization conducts and the resources used by the program. Outcome measures are particularly useful because they indicate what program activities are accomplishing. At the time of our November 2004 report, agencies were only in the early stages of implementing security performance measures.

The need to better protect federal facilities, coupled with federal budget constraints and the increased scrutiny of homeland security funding and programs, has prompted the need for U.S. agencies to measure the performance of their facility protection efforts. In this environment, it is important for these agencies to ensure that investments in facility protection are providing adequate returns in terms of better protecting real property assets against terrorism. In addition, the U.S. government's national strategy, Presidential directive, and guidance on protecting critical infrastructures—including facilities—have identified the use of performance measurement as a key means of assessing the effectiveness of protection programs. Given that protection of critical infrastructures is an important issue for organizations outside of the federal government as well, it is beneficial to look to the experiences of these organizations to identify lessons learned. As such, our objectives for this review were (1) to identify examples of performance measures for facility protection being used by selected organizations outside of the federal government—including private-sector entities, state and local governments, and foreign governments, and (2) to determine the status of U.S. federal agencies' efforts to develop and use performance measures as part of their facility protection programs. To address the first objective, we interviewed private-sector representatives from four entities in the gaming industry and from five major financial services entities, because these industries were identified as having invested in security and likely to have developed performance measures. We also interviewed officials from 17 of the 20 state and local governments that received the most funding from two

⁷Performance measurement is the ongoing monitoring and reporting of program accomplishments, particularly progress toward preestablished goals. It is typically conducted by program or agency management.

security-related DHS grant programs in fiscal year 2005.⁸ Finally, we interviewed government officials from multiple agencies in Australia, Canada, and the United Kingdom, because these countries have experience with threats of terrorism and have performance measurement initiatives. We also reviewed relevant documents we obtained from these organizations, related GAO reports, and literature on performance measurement. To address the second objective, we interviewed federal officials from DHS, GSA, USPS, VA, and Interior—the agencies that hold, or are responsible for the security of, the majority of the domestic, nonmilitary property. We also reviewed pertinent documents and policies obtained from these agencies, in addition to related laws and directives. A detailed discussion of our scope and methodology, including more information on how we selected the organizations we contacted, is contained in appendix I. We conducted our work between June 2005 and April 2006 in accordance with generally accepted government auditing standards.

Results in Brief

We found a range of examples of performance measures that organizations outside the U.S. government, including private-sector firms, state and local governments, and foreign government agencies, use to help improve the security of facilities, inform risk-management and resource-allocation decisions, and hold security officials and others in their organizations accountable for security performance. These included output measures, such as the average time to process background screenings, and outcome measures, such as the change in the total number of security incidents relating to thefts, vandalism, and acts of terrorism. For example, an agency in Australia monitors an outcome measure concerning the impact of additional security expenditures on a facility's risk rating, while controlling for existing security enhancements that mitigate the risk, such as the number of guard patrols and the adequacy of access control systems (e.g., electronic locks). In another example, each business line in one financial services organization conducts security compliance reviews of its facilities, including confirming the presence of required key security equipment and determining whether staff are following security policies. Senior security officials review the results to determine where problems exist and hold each business manager accountable for addressing them. Despite some organizations' use of these measures, less than one-quarter

⁸Of the 20 state and local governments we attempted to contact, we were able to obtain information from officials from 17 of them.

of the organizations we contacted had developed performance measures for facility protection, and there was widespread acknowledgement among the organizations that effectiveness in facility protection is challenging to measure. For example, security officials do not necessarily know whether a potential security threat or incident has been prevented, even after perceived security weaknesses have been addressed. Since security is so challenging to measure, some of the organizations that we interviewed told us that they rely on U.S. federal agencies for support and leadership in developing security standards and performance measures, and one foreign government agency said it was interested in developing guidance for security performance measurement but was looking to U.S. federal agencies for assistance in this area.

We found that some bureaus and services within three of the agencies we reviewed—DHS (for GSA properties), USPS, and Interior—are using output measures, and, to a lesser extent, outcome measures, while VA and some bureaus and services within the other three agencies are not. The agencies that have developed performance measures use them to evaluate and improve program effectiveness, make risk management decisions, and help ensure adequate protection at individual facilities. For example, within DHS, FPS has established an output-oriented performance measure to monitor the timely deployment of security enhancements such as x-ray machines. Such a measure provides a basis for FPS to compare planned versus actual performance. Several bureaus and services within USPS and Interior have developed methodologies to rank and monitor the relative risk ratings of their respective facilities over time—these ratings are then used as outcome measures for determining the change in the effectiveness of facility protection efforts. VA and the bureaus and services that did not have security performance measures generate data on ongoing protection activities, such as monitoring the numbers and types of security breaches at a given facility. This information could provide useful feedback about the agency's effectiveness in mitigating building security risks and therefore could be used for measuring performance. Although agencies have placed an emphasis on performance measurement and initiatives are under way, agency security officials said it has been challenging to measure the actual impact of various approaches on improving security and that resources for measurement initiatives have been scarce. Furthermore, while importance has been placed on performance measures in national homeland security policies and broad guidance exists for measuring the performance of critical infrastructure protection programs, agencies have not established specific guidance and standards for developing and using performance measures for facility protection programs in particular. This differs from the information technology

security area, where agencies not only are required to measure performance, but also have detailed guidance and standards for developing and implementing performance measures. Without effective performance measurement data, especially data on program outcomes, decision makers may have insufficient information to evaluate whether the benefits of security investments justify their costs, to determine the effectiveness of security activities, to know the extent to which security enhancements have improved security or reduced federal facilities' vulnerability to acts of terrorism or other forms of violence, or to determine funding priorities within and across agencies.

Because ISC was established to enhance the quality and effectiveness of security in buildings and facilities in the United States and to provide a permanent body to address continuing governmentwide security in federal facilities, we are recommending that the Secretary of DHS direct ISC to (1) establish guidance and standards for measuring the performance of facility protection efforts, particularly for program outcomes; (2) communicate the established guidance and standards to relevant federal agencies; and (3) ensure that the guidance and standards are regularly reviewed and updated. In commenting on a draft of this report, DHS, USPS, VA, and Interior generally concurred with the findings, and DHS concurred with the recommendations. DHS, USPS, and Interior also provided comments, which were incorporated as appropriate to ensure accuracy. GSA said they did not have any comments on the draft report.

Background

The protection of federal facilities gained importance after the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, and this issue became even more critical after the 1998 embassy bombings in Africa; the September 11, 2001, attacks on the World Trade Center and the Pentagon; and the anthrax attacks in the fall of 2001. Shortly after the 1995 bombing, the President signed Executive Order 12977, establishing the Interagency Security Committee (ISC). ISC—which has representation from all major federal departments, agencies, and key offices—was charged with enhancing the quality and effectiveness of security in, and protection of, nonmilitary facilities occupied by federal employees in the

United States.⁹ Furthermore, ISC was tasked to serve as a permanent body to address continuing governmentwide security issues for federal facilities. Under the order, ISC became responsible for developing policies and standards, ensuring compliance and overseeing implementation, and sharing and maintaining information. Around the same time that ISC was created, the Department of Justice categorized all federal facilities into security levels I through V based on factors such as facility size and number of employees, and it established recommended minimum security standards for each of the five levels. These standards covered perimeter, entry, and interior security and security planning.¹⁰

The 2001 terrorist attacks prompted additional policies concerning facility protection and a variety of security enhancements at federal facilities. The Homeland Security Act of 2002 and a number of national strategies, including the National Strategy for Homeland Security,¹¹ assigned DHS specific duties associated with coordinating the nation's efforts to protect critical infrastructures and key assets. Government facilities (at the federal, state, and local levels) were identified as key assets and therefore were included in this effort.¹² Furthermore, the 2002 Act transferred FPS from GSA to DHS and, as a result, made DHS responsible for ISC.¹³ A related directive, the Homeland Security Presidential Directive Number 7

⁹ISC membership includes the Departments of State, Treasury, Defense, Justice, Interior, Agriculture, Commerce, Labor, Health and Human Services, Housing and Urban Development, Transportation, Energy, Education, and Veterans Affairs; GSA; Environmental Protection Agency; Central Intelligence Agency; and the Office of Management and Budget. Other members of ISC include the Director, U.S. Marshals Service; the Director, Security Policy Board; and the Assistant to the President for National Security Affairs. As a member of ISC, the Department of Defense participates in meetings to ensure that its physical security policies are consistent with ISC security standards and policy guidance, according to the Executive Director of ISC.

¹⁰U.S. Department of Justice, *Vulnerability Assessment of Federal Facilities*, June 28, 1995.

¹¹Office of Homeland Security, *The National Strategy for Homeland Security*, July 2002.

¹²The other critical infrastructure sectors and key assets identified in the *National Strategy* include agriculture and food, water, public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, national monuments and icons, nuclear power plants, dams, and key commercial assets.

¹³Executive Order 13286, dated February 28, 2003, amended numerous executive orders to reflect the transfer of certain functions and responsibilities to the Secretary of Homeland Security. Section 23 of the Executive Order transferred the ISC chairmanship responsibility from GSA to DHS.

(HSPD-7), stated that DHS's Secretary was responsible for coordinating the overall national effort to identify, prioritize, and protect critical infrastructures and key assets.¹⁴ To meet this responsibility, DHS developed a National Infrastructure Protection Plan (NIPP), which is currently in draft form. FPS is responsible for implementing the NIPP for the government facilities sector. HSPD-7 also required each federal agency to develop plans to address identification, prioritization, protection, and contingency planning for physical and cyber critical infrastructures, along with key assets that they hold or operate. As the governmentwide emphasis on protecting critical infrastructures mounted, the federal agencies' facility protection efforts continued to intensify. In addition to implementing such activities as searching vehicles that enter federal facilities, restricting parking, and installing concrete bollards, federal agencies also implemented various security technologies, such as smart cards for access control. Figure 1 shows smart card technologies that are utilized at a federal building.

¹⁴Homeland Security Presidential Directive Number 7, *Critical Infrastructure Identification Prioritization and Protection*, Dec. 17, 2003.

Figure 1: Smart Card Access Portals at a Federal Building Entrance



Source: GAO.

While it is evident from the policies and strategies outlined above that the protection of key assets, including federal facilities, has become an important issue for the U.S. government, the protection of such assets has also gained attention in state, local, and foreign governments, as well as the private sector. State and local governments in the United States, for instance, have taken steps to ensure the protection of critical infrastructures and key assets within their jurisdictions, often receiving resources for such efforts from the federal government. For example, DHS's Homeland Security Grant Program provides funding to state and local governments to prevent, deter, respond to, and recover from acts of terrorism. Funding from this grant program can be used for, among other

things, critical infrastructure protection activities. The protection of critical infrastructures and key assets has also gained momentum in foreign governments, particularly in countries like the United Kingdom that have recently faced terrorist attacks. Furthermore, because many U.S. critical infrastructures are owned and operated by the private sector, and because some of these infrastructures have been targeted by terrorists in the past, many private-sector entities have increased their investments in security efforts.

Due in part to the growing attention to facility protection, we designated federal real property as a high-risk area in January 2003 and have since published a number of reports on this issue.¹⁵ In a November 2004 report, we identified six key practices in protecting federal facilities, one of which was measuring performance to help achieve broad program goals and to improve security at individual facilities. We reported that, for broader program goals, performance measures could indicate whether organizations establish timelines and adhere to budgets. And, at the individual facility level, on-site security assessments and other active testing could provide data on the effectiveness of efforts to reduce a facility's vulnerability to attack. Training exercises and drills are also useful in assessing preparedness.¹⁶

The need for agencies to measure performance stemmed from the Government Performance and Results Act of 1993 (GPRA),¹⁷ which was intended to improve federal program effectiveness, accountability, and service delivery. This act required federal agencies to develop strategic plans, link them with outcome-oriented goals, and measure agency performance in achieving these goals. Likewise, in the security context, a number of national strategies called for federal agencies to use performance measures to, among other things, assist in the planning and budgeting of protection activities for critical infrastructures and key assets.

We have previously reported that successful performance measures should (1) be linked to an agency's mission and goals; (2) be clearly stated;

¹⁵For example, see GAO, *High-Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005); [GAO-05-790](#); and [GAO-05-49](#).

¹⁶[GAO-05-49](#).

¹⁷Pub.L. No. 103-62, 107 Stat. 285 (1993).

(3) have quantifiable targets or other measurable values; (4) be reasonably free of significant bias or manipulation that would distort the accurate assessment of performance; (5) provide a reliable way to assess progress; (6) sufficiently cover a program's core activities; (7) have limited overlap with other measures; (8) have balance, or not emphasize one or two priorities at the expense of others; and (9) address governmentwide priorities.¹⁸

Managers can use performance measures in a number of ways to improve programs and allocate resources more efficiently and effectively. Decision makers can use results from performance measurement to identify problems or weaknesses in programs, identify factors causing the problems, and modify services or processes to try to address problems. Conversely, results from performance measurement can be used to identify and increase the use of program approaches that are working well and to consider alternative processes in areas where goals are not met. Separately, performance measures can also be used to identify priorities and allocate resources. Decision makers can compare performance measure results with program goals and subsequently determine where to target resources to improve performance. Furthermore, in a risk management process, agencies can use performance measurement to assess progress towards meeting homeland security goals. The intended effect of assessing such progress, when coupled with other aspects of the risk management process, is the reduction of risk.¹⁹ Finally, when performance information is used to reward individuals, these measures can hold individuals accountable for certain work activities and related goals and, as a result, create an incentive for achieving results. A greater focus on performance results can be achieved by creating a cascade from an organization's goals and objectives down to the individual performance level. Such alignment facilitates the linking of individual performance to organizational performance.²⁰

¹⁸See GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, [GAO-03-143](#) (Washington, D.C.: Nov. 22, 2002), pp. 2-3, 46-53.

¹⁹GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, [GAO-06-91](#) (Washington, D.C.: Dec. 15, 2005), pp. 24, 105.

²⁰See GAO, *Managing For Results: Enhancing Agency Use of Performance Information for Management Decision Making*, [GAO-05-927](#) (Washington, D.C.: Sept. 9, 2005), pp. 7-17 and 21.

Organizations outside of the U.S. Government Use Security Performance Measures to Enhance Decision Making and Help Ensure Accountability

We found a range of examples of performance measures that organizations outside the U.S. government—including private-sector firms, state and local governments, and foreign government agencies—used to track the number and types of security activities conducted, the quantity of security equipment and services delivered, and the outcomes of these security efforts.²¹ Security officials within these organizations recognized that performance measures helped them better assess how effective they were in protecting against threats to and vulnerabilities of their facilities. Organizations then used the results of these performance measures to improve security, inform the risk management process, make resource allocation decisions, and hold security officials and others in the organization accountable for security performance. Despite efforts by some organizations to use performance measures as an additional decision-making tool, some security officials told us that they faced some challenges in developing and implementing performance measures. The challenges include limited guidance and expertise in the performance measurement area.

Selected Organizations Use a Range of Output, Outcome, and Process/Input Measures to Assess the Effectiveness of Facility Protection Efforts

Security officials recognized that performance measurement is important for improving facility protection and ensuring accountability. They also acknowledged that performance measures would allow them to take a more strategic, outcome-based approach to managing their security programs and to better prepare their facilities against terrorism and other threats. However, less than a quarter of the organizations we interviewed told us that they have developed and used various performance measures for their security programs, and several of those that did have performance measures said that the measures are still a work in progress. Table 1 provides examples of the output, outcome, and process/input measures these organizations have developed. Appendix II provides additional examples of performance measures.

²¹For this report, we categorized the District of Columbia as a local government.

Table 1: Examples of Performance Measures for Facility Protection

Type of measure	Example
Output	• Number of risk assessments performed • Average time to process background screenings • Compliance with security policies • Client/customer satisfaction with security services
Outcome	• Evidence of damage to buildings and facilities • Change in risk rating resulting from countermeasures deployed • Change in the total number of security-related incidents
Process/Input	• Number of security clearances undertaken • Number of training courses and drills conducted • Number of security guards

Source: GAO.

Note: GAO analysis of data from selected state, local, and foreign government agencies and private-sector organizations.

In some of the organizations we interviewed, some security officials use output measures to monitor the direct products and services delivered by a program and the characteristics of those outputs, including efficiency, cost-effectiveness, timeliness, quality, and customer service. Some security officials use outcome measures to compare the results of those products and services with the goals security officials are trying to achieve, such as reducing the total number of security incidents relating to thefts, vandalism, and acts of terrorism. In addition, some security officials use outcome measures to assess whether their security program is operating efficiently and to determine the quality of the services and products they are trying to provide. Separately, security officials use various process/input measures to provide a descriptive overview of the program activities and the resources of their security program, including the types and numbers of facilities they manage and the level of countermeasures,²² such as entry control security systems, they have installed. Input measures are used for resource allocation and monitoring and do little to reflect the effectiveness of the security program.

As an additional output measure, some of the organizations we interviewed determine whether their security efforts comply with their security policies, standards, and guidance. For example, some of the

²² A countermeasure is any action taken or physical equipment used principally to reduce or eliminate one or more vulnerabilities.

government agencies in the three foreign countries we visited use performance measures to evaluate whether their security activities are compliant with their government's protective security policies. Several security officials in these agencies told us that they use this measure to demonstrate compliance with established government standards. Some of these foreign government agencies indicated that they measure compliance based on the results of security audits completed internally—by the security department or other departments within the organization—or externally. Some of these security officials then use the results of the audits to identify security weaknesses and make corrections to improve security. Other foreign government agencies use surveys to measure the degree of security policy compliance. For example, Australian government agencies are required to adhere to the minimum protective security standards contained in the Australian government's Protective Security Manual.²³ Ministers and agency heads are accountable for their agency's compliance with these standards. Agencies are surveyed annually for compliance with the security manual standards. The survey results are assessed and reported to the central government.

Some of the nonfederal organizations we interviewed also measure the effectiveness of their countermeasures by determining whether the services and security equipment they provide are adequate under both real and simulated conditions. Some of the organizations we interviewed stated that they test security equipment, such as perimeter alarms and x-ray machines, and conduct simulated attacks and penetration exercises on a periodic basis. One official from the gaming industry said that it is important to test equipment to ensure it is being used properly, because the technology itself is not as important as how it is used. For example, a facility could have a sophisticated card access system but still be vulnerable if someone props the door open. To help government agencies select effective security equipment, a central agency in the United Kingdom tests security equipment and provides those in the security community with information to help the user match the appropriate equipment to the requirement. Similarly, an agency in Australia conducts tests on security equipment and provides agencies with a catalog of approved products. Security officials from the gaming industry also told us

²³The Australian government's Protective Security Manual contains governmentwide policies and guidelines that establish the minimum standards for the protection of Australian government resources (including information, personnel, and assets) that all agencies governed by the country's *Financial Management and Accountability Act of 1997* must meet.

that they are members of an external group that tests security equipment and shares the results of the testing with security officials in other industries, such as the chemical, petrochemical, and pharmaceutical industries.

In some organizations, the selection of useful performance measures has evolved through a trial-and-error process. For example, one financial services organization went through several iterations of its security performance measures over a 1-1/2 year period in order to determine which performance measures were important to monitor and would provide them the right information needed to achieve the organization's security objectives. For example, they initially reported on the number of security alarms, and then changed the measure to a more useful measure—the number of alarms with unique responses (i.e., alarms that required a guard to respond in person)—so that they could better understand how security staff were interacting with the security equipment. One security official acknowledged that, although they were satisfied with their current performance measures, it would still be helpful to measure performance in other areas, such as employee satisfaction with security services.

Case Example: A Financial Service Organization's Performance Measures

Security officials at a large, well-known financial services organization use a number of output and outcome measures to regularly monitor the performance of their security program. In addition, they use process/input measures to assist them with resource allocation decisions. The security officials emphasized that there is a constant need to measure and evaluate what their security program does in order to educate business professionals on the importance of a security investment. While the organization assesses all of its facilities using a baseline set of security standards and risk assessments, performance measures provide security officials with information to understand whether these standards and risk assessments are actually improving their security situation. The security officials told us that they use the following performance measures:

- *Outputs*—Security officials use output measures relating to their operational readiness (i.e., how prepared the security program is against potential security threats), which includes the number of risk assessments performed. They also measure the number of non-security related incidents such as false alarms or broken security cameras. In addition, security officials monitor the number of policy exceptions that exist when a business line or facility cannot comply with the standards set forth in their security policy manual. If many exceptions to a particular section of the policy manual occur in a given month, a policy working group reviews

the issue and determines whether additional assistance will be required to bring the facilities into compliance.

- *Outcomes*—One outcome measure is the monetary savings resulting from less costly, more efficient security processes and new technologies. Security officials use this outcome measure to demonstrate savings from the security program's budget as well as from the budgets external to the security division, such as operations. Officials are also able to prorate contract-related savings over the lifetime of the contract to better understand how the savings affect the organization over time. To understand the effectiveness of their security efforts, security officials use data on the responses to security incidents, which are classified by type (e.g., assault, burglary, terrorism). Security officials then analyze the data to help them make recommendations for additional security improvements.
- *Process/Input*—The financial organization tracks guard levels, security expenditures, and security activities across all its facilities. Security officials use these measures to compare the different levels of service required, given the risk associated at each facility or region. In a given month, they also measure the number of training sessions and drills conducted. The performance measure for training identifies the specialized fields in which the security staff are being trained and the type of training the security staff are providing to others.

Security officials at this financial services organization told us that they monitor their performance measures on a monthly basis, and that the data are aggregated for the entire organization and also broken out by region. They developed, and have continued to modify, their performance measures based on the analysis of incidents and other activities in a particular region as well as trends across regional facilities. They also obtained feedback from regional offices and from their own security staff. Security officials noted that they tried to select performance measures that represented common threads and were not biased in favor of one particular region. They also continuously evaluate the usefulness of their performance measures, adding a measure if they determine that information is needed on a particular subject or dropping a measure if it does not seem to be informative.

Security Officials Use Performance Measure Results for Risk Management and Resource Allocation

We have previously reported that organizations can use the results of performance measures to make various types of management decisions to improve programs.²⁴ Security professionals also recognize the benefits of using performance measurement within the security industry. At a major security industry conference in 2005, a conference presenter indicated that the ability to compare past performance and the performance of others contributes to the goal of continuous improvement, the result of which is a stronger, more mature security program with security processes that can better protect facilities and staff from harm. Performance measures also provide management with the tools to verify that the organization's resources are used responsibly and security risks are managed appropriately.

In some of the organizations we interviewed, security officials and other decision makers use performance measures to manage risk, allocate resources, and improve the quality of the security services they provide for their facilities. For example, at one financial services organization, security officials installed protective security equipment at some of their facilities and then compared the number of security incidents and the level of customer satisfaction before and after the equipment was installed. In this particular case, security officials used this performance measurement data to demonstrate the value of that security investment to their corporate management and the business lines they supported. The performance measures also allowed security officials to compare individual facility performance to the average within the industry, which they use to demonstrate the risk level of a particular facility and take appropriate action to address the risk.

Where security goals and objectives were not achieved, some security officials also used performance measurement results to identify problem areas and take corrective action. Several organizations mentioned that they measure the quality of their security efforts through an output measure by soliciting feedback from employees and clients through customer satisfaction surveys. For instance, one Canadian organization periodically surveys clients about their satisfaction with the security services the organization provides to government agencies. The survey questions range from how often the client saw security managers to how satisfied they were with the services they received. The responses to the

²⁴See [GAO-05-927](#).

surveys provide feedback that allows security officials to improve their provision of security services to both private and public sector clients.

Case Example: An Australian Agency's Risk Model

Performance measures helped security officials in one government agency in Australia become better risk managers and allocate resources more efficiently across facilities. The agency uses a security plan that includes security objectives that are linked to its strategic goals. The plan also lists strategies and actions for achieving these objectives, along with performance measures that assess the extent to which objectives are being achieved. For example, the performance measures monitor the extent to which security practices are in accordance with the agency's security policies, any evidence of harm to agency staff or facilities, and the extent to which agency stakeholders view the agency's facilities as safe for their resources and assets. To monitor performance, security officials use two different review processes. First, security officials can access the audit function of a computer-based risk assessment model to monitor the outcomes of the performance measures contained in their security plan and to understand how well their security efforts are performing within individual facilities. For example, the risk-assessment model allows security officials to monitor the impact of additional security expenditures on a facility's risk rating while controlling for existing security enhancements that mitigate the risk, such as the number of guard patrols and the adequacy of access control systems (e.g., electronic locks). Security officials can then use the results to justify spending decisions and prioritize security investments. For example, one facility requested a perimeter fence, and security officials were able to use the risk-assessment model to demonstrate that the facility's risk was adequately managed without the fence since there were no known risks in that location and since the facility already had guards and an alarm system. Second, the agency's audit unit also conducts its own independent measurement of the security activities so that security officials can compare across facilities to guide them in determining where they need to make adjustments. Together, these two security reviews provide the security program with enough information to assess their security position, according to one agency security official.

Performance Measures Can Be Used to Hold Security Officials Accountable for Achieving Goals and Results

Security officials recognized the value of performance measures to help ensure the accountability of security officials, management, and other employees throughout the organization. Many of the organizations we interviewed had security policies and procedures in place, and some of these organizations were able to link these plans directly to performance measures that demonstrated achievement of both the security-related

Case Example: The District of Columbia's Alignment of Security Goals and Measures

strategic goals and the organization's broader strategic goals. We have previously reported that aligning the goals at the executive level with the goals and objectives at each operational level reinforces the connection between strategic goals and the day-to-day activities of managers and staff.²⁵ For example, an annual goal that is linked to a program and also to a long-term goal can be used to hold agencies and program offices accountable for achieving those goals.²⁶ Furthermore, we reported that such alignment increases the usefulness of performance information to decision makers at each level.²⁷

One agency within the District of Columbia (D.C.) government uses performance measures and targets to hold agency management and security officials responsible for its security-related activities. D.C.'s Office of Property Management is responsible for D.C. government buildings, and the Protective Services Division, which falls under Property Management, is responsible for security at these buildings. Protective Services faces a unique environment in protecting the facilities that it is responsible for because of the proximity of these assets to federal facilities, which are considered to be attractive targets for terrorist attacks. To help ensure that their security concerns are addressed, security officials in Protective Services noted that they have linked their security goals and related performance measures with the Property Management's goals and citywide strategic goals (see fig. 2). Specifically, Protective Services' goals, performance measures, and related targets support the goal of Property Management to provide a high-quality work environment and user-friendly facilities, and also support the broader citywide strategic goal of making government work. The security officials pointed out that this alignment is very deliberate and can help hold officials accountable for a security-related activity. For example, the Director of Property Management can use security-related performance measures and corresponding targets to hold the Protective Services Division accountable for its activity. If Protective Services does not meet the targets, it is required to submit justifications to senior management as to why they were not met. The officials explained, however, that in situations where there are unforeseen circumstances, their targets can be realigned, with the consent of senior management. For example, following Hurricane Katrina, Protective

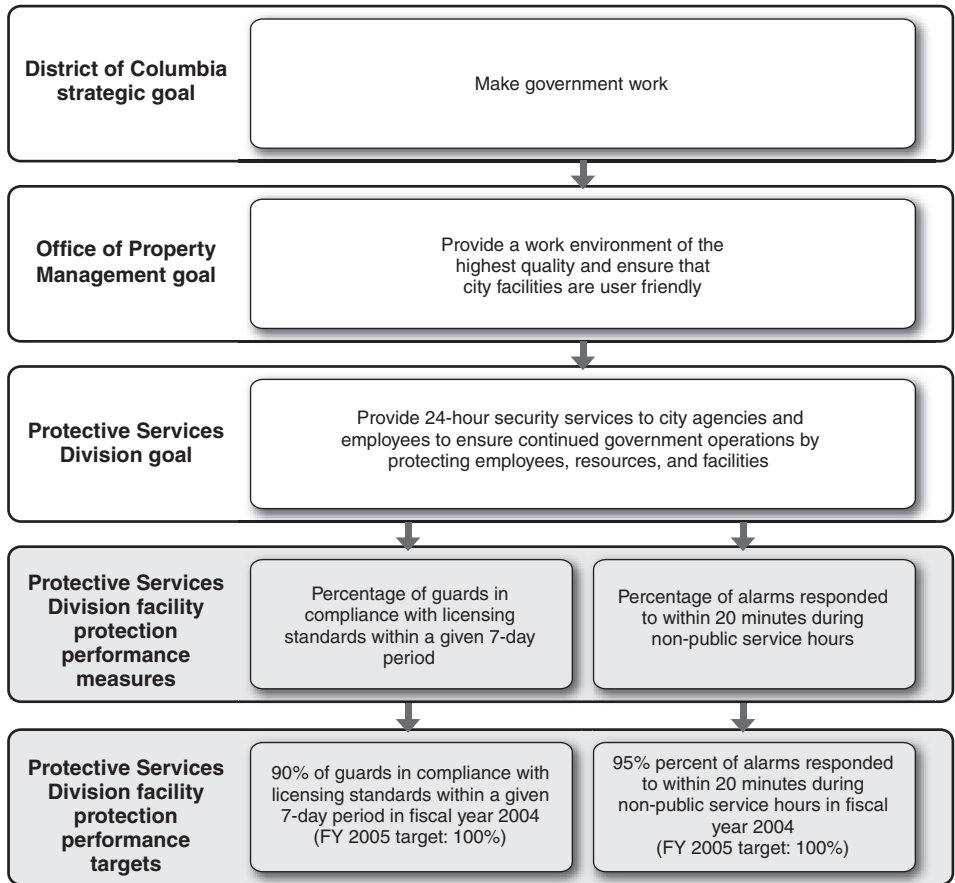
²⁵ [GAO-05-927](#).

²⁶ [GAO-03-143](#).

²⁷ [GAO-05-927](#).

Services was required to provide security services for Katrina victims housed at a D.C. arena. The human resources required for this task made it impossible for Protective Services to meet all the targets, and the D.C. mayor's office allowed for adjustments to the target for that time. Separately, the mayor's office can also use the security-related performance measures and targets in conjunction with other Property Management performance measures and targets to monitor the work of the entire agency and hold the Director of Property Management accountable for agencywide activity.

Figure 2: Linkages between District of Columbia Strategic Goals and Performance Measures for Facility Protection



Source: GAO analysis of District of Columbia data.

large numbers of mission-critical facilities.²⁸ Such a high-level position is important for coordinating security responsibilities across facilities and ensuring accountability for security results, including establishing linkages between security performance and outcomes. We found that government agencies in all three countries we visited are required to designate a departmental security officer (DSO) or an agency security executive to oversee security matters across all agency facilities and implement government security policies. For example, in the United Kingdom, security officials told us that the DSOs are sufficiently senior within each agency department to have an effective voice and to put security issues on the management agenda. These security officials also told us that the DSOs are playing a greater role in coordinating with other agency departments to enhance their security. The financial services and gaming organizations we interviewed also have directors or vice-presidents of security who have a direct line of communication to their corporate management. They said that this arrangement promotes a good working relationship with management and allows them to identify and fix security problems efficiently.

Some of the organizations we interviewed also used performance measures to hold security officials accountable for program performance. For example, some organizations hold their security officials accountable for results through the use of customer satisfaction surveys. Security officials at one financial services organization indicated that they conduct quality surveys with their business-line clients, which allows clients to provide input to security officials on whether the security program is effective and whether the security program met the client's expectations.

Case Example: Individual Accountability in Two Financial Services Organizations

Two major financial services organizations we interviewed use performance measures to help ensure accountability for investments in security improvements and compliance with security policies and regulations. Security officials in one financial services organization told us that they work in a security culture that is very performance driven. While their security budget is fully separate from other corporate expenditures, regional security directors are responsible for determining how to spend security funds. Regional security directors use performance measures to justify security expenditures to all of the individual business lines they support and to demonstrate a return on investment for their security expenditures. For example, the organization uses output and outcome

²⁸ [GAO-05-790](#).

performance measures to monitor monetary savings, the number of security incidents, and the impact of new technologies and processes. When security officials want to invest in a new security technology, they use these performance measures to demonstrate to the business lines that they have investigated all of the alternatives and determined the cost and potential savings of the purchase. For example, they used past data on the cost and performance of security equipment and guards to calculate the cost of installing some security equipment versus hiring a security guard to protect one of its facilities. They were able to demonstrate that the security equipment would be more cost-efficient over time and be more effective in deterring certain crimes.

Another financial services organization uses performance measures to help ensure that all facilities are complying with its security policies and regulations. The security policies for each of the organization's business lines differ based on their level of risk. As a form of quality control for its security operations, each business line is expected to conduct compliance reviews of all of its facilities, including confirming the presence of required key security equipment and determining whether staff members are following security policies. Each business manager is held accountable for the results of these reviews: senior security officials receive and review monthly compliance reports, and the financial services organization's central audit department ensures that the reviews were properly conducted. According to security officials, the data in the monthly reports are used to determine where problems exist and look for emerging security trends.

Case Example: An Australian Agency's Security Certification Process

One Australian government agency uses performance measures to hold its security executives accountable for identifying and addressing security risks. Officials from the agency noted that they have historically had a strong security and risk management culture that emphasizes executive accountability for performance. The agency holds its security executives accountable by requiring them to produce a certificate of assurance that includes physical and personal security. The purpose of the certificate, which is signed by a senior agency executive, is to assure the chief executive that the agency is meeting its security obligations, and that action plans are in place to address any problems. It covers compliance with external requirements, including government regulations, and internal conformance with corporate security policies. The assurances given must be underpinned by evidence, which includes the results of physical security reviews that are conducted periodically at each facility. These reviews measure and report on the standard of physical security, including perimeter security, access control, alarm systems, and

surveillance and communication systems. The certificate uses a color code to indicate the overall status of the security function—red, amber, or green. Certificates rated red or amber are reviewed and resubmitted every 6 months. Green certificates are reviewed annually. If the certificate identifies a security problem, it must be accompanied with an action plan for addressing the risks involved.

Organizations Cited Challenges in Developing and Using Performance Measures

Although performance measurement is seen as an important tool for assessing the effectiveness of security programs, developing and using performance measures can be challenging, according to security officials we interviewed at selected organizations. A difficulty with developing performance measures is determining whether the measures that are used are suitable, given a constantly changing threat environment. Some security officials said that it was difficult to know what to measure because security is intangible or difficult to quantify. Others also acknowledged that it is difficult to determine whether a potential security threat or incident has been prevented, even after additional countermeasures or security staff are introduced to address perceived security weaknesses, because deterrence is immeasurable. Several security officials cited the difficulty in determining a causal relationship between security efforts and changes in the number of security incidents. For example, a security official from an Australian government agency indicated that an increase in the number of breaches in a particular facility may result because an organization is being targeted at that particular point in time rather than because it lacks adequate security measures. Organizations also find it hard to measure the impact of some security actions, such as the potential financial savings resulting from attacks that have been discouraged. Organizations told us that they recognize the need to draw linkages between security incidents and security investments, but some organizations find it difficult to measure the benefit of a particular security process or piece of equipment in the absence of a security breach.

A number of organizations also told us that other priorities and considerations might hinder their ability to effectively use performance measures for making security decisions. Some security officials pointed out that the ultimate decision on how to allocate security resources can be based on priorities other than performance. For example, several private sector and foreign government agencies we interviewed noted that they have to balance their security needs with their goals of maintaining sufficient public access to their facilities. Some security officials are also reluctant to use performance measures because they do not want to be held accountable for not meeting their performance targets. Several

organizations mentioned that potential liability could be seen as a disincentive for using performance measurement data, because an organization may be seen as negligent if the performance data were to show that an organization could have done something to prevent an incident but chose not to. One security official told us that having established performance targets could also discourage organizations from accurately collecting data because security officials may be reluctant to report an incident if a decline in the number of incidents is one of the performance goals.

Some organizations we interviewed cited the lack of knowledge and expertise available to collect and analyze security data as a limitation to overcoming some of the challenges of using performance measures. One financial services organization indicated that some of its security officials did not see the benefits of using performance measures until after they saw that their business line managers responded favorably to the use of performance measures to demonstrate a return on investment for security expenditures. Several state, local, and foreign government agency officials noted that they had limited management staff available to develop and monitor performance measures for physical security. According to one state government agency official, without staff expertise in this area, security staff tend to approach security initiatives like a project—they monitor the initiative’s progress to make sure that it is delivered on time and on budget, but they do not necessarily measure the effectiveness of the security equipment once it is installed.

Many organizations we interviewed said that they face the aforementioned challenges, and we noted that some of the entities outside the U.S. government rely on U.S. agencies for support and leadership in developing security standards and performance measures. One state government agency we interviewed expressed an interest in developing performance measures in the future and mentioned that it often looks to the federal government for guidance on security efforts. DHS officials told us that their agency was providing assistance to several foreign government agencies in the United Kingdom in measuring performance and allocating security resources. One foreign government agency said that it was interested in developing governmentwide guidance for measuring security performance but was looking to U.S. agencies for assistance in this area.

U.S. Agencies Have Made Some Progress in Developing and Using Performance Measures for Facility Protection Programs, but Lack Guidance and Standards

Responding to the requirements in 2002 by the National Homeland Security Strategy and subsequent federal policies, agencies have paid greater attention to facility protection and have begun using key practices—such as performance measurement—to varying degrees. Agency officials noted that developing performance measures for facility protection was a difficult undertaking, since the results are not always readily observable. We found that some bureaus and services within three of the agencies we reviewed—DHS, USPS, and Interior—are using output measures and, to a lesser extent, outcome measures, while the VA and some bureaus and services within the other three agencies are not. Despite the lack of security performance measures, we found that ongoing protection activities within these bureaus and services and the VA, such as monitoring the numbers and types of security breaches at a given facility, generate a wealth of data that could provide useful feedback about the agency's effectiveness in mitigating building security risks, and therefore could be used as measures of performance. While the agencies have demonstrated some progress in applying performance measurement to facility protection, with limited precedent for how to do this, more work remains to identify measures—particularly outcome measures—that assess the impact of facility protection efforts. Output measures do not provide an indication of what security activities are accomplishing, while outcome measures that are clearly tied to results indicate the extent of progress made and help identify the security gaps that still remain. Officials expressed concerns about the lack of resources and the limitations of existing guidance in providing direction about how to measure progress and evaluate the effectiveness of physical security programs.

Agencies Use Output Measures and Some Outcome Measures to Inform Risk Management, Help Ensure Adequate Protection, and Assess Effectiveness of Facility Protection Efforts

In general, the agencies we reviewed have made some progress in collecting and using performance-related data for their facility protection program activities, but many of the measures are of program outputs rather than outcomes. While output measures are an important part of performance measurement, outcome measures could provide information to evaluate whether the benefits of security investments outweigh their costs and to determine the effectiveness of security activities. The agencies we reviewed use output measures, such as the timely completion of risk assessments and whether countermeasures work as intended once deployed, to inform risk management decisions and to help ensure adequate protection at the individual facility. Additionally, several bureaus and services within DHS, USPS, and Interior have developed outcome measures to rank and monitor the relative risk ratings of their respective

Case Example: DHS's Federal Protective Service in GSA Facilities

facilities over time or to otherwise assess the effectiveness of their facility protection efforts.

The effectiveness of security programs at GSA facilities is evaluated using performance measures developed by the Federal Protective Service (FPS) and a physical security testing program developed by GSA. FPS has identified four performance measures—both output and outcome measures—to assess its efforts to reduce or mitigate building security risks. These four performance measures, detailed in table 2, are at varying stages of implementation and are still evolving. Under the Homeland Security Act of 2002, DHS, through FPS, is directly responsible for law enforcement and security-related functions at facilities under GSA's control or custody. FPS delivers security and law enforcement services for approximately 8,000 facilities that fall under GSA's jurisdiction.

Table 2: FPS's Performance Measures for Facility Protection

Type of measure	Performance measure	Purpose
Output	Timely deployment of countermeasures	To compare actual deployment dates with planned deployment dates
Output	Countermeasure functionality (e.g., surveillance cameras, x-ray machines)	To gauge whether those security countermeasures for which FPS is contractually responsible are working as intended, once deployed
Output	Patrol and response time	To assess FPS's ability to respond to calls for service within certain time limit goals
Outcome	Facility security index	To calculate FPS's average success rate for the above three performance measures

Source: GAO.

Note: GAO analysis of FPS data.

The first measure—monitoring the deployment of countermeasures—focuses on the timeliness of implementation and serves as a measure of program output. Once approval and funding have been obtained to implement a recommended countermeasure, FPS personnel record planned deployment dates so that they can compare them with actual implementation dates. An FPS working group decided that the initial baseline for this measure, developed in fiscal year 2005, would be 90-percent success, which is calculated as the number of countermeasures actually deployed by the scheduled due date, divided by the number planned. FPS officials noted that they will not know how well they are progressing on this measure until the end of fiscal year 2006 because they are still automating the process and training regional staff. For fiscal year

2007 and subsequent years, FPS expects the annual goal to be some increment above the preceding year's results until the long-term goal of 98 percent is achieved and maintained.

Countermeasure functionality, FPS's second measure, gauges whether a countermeasure works as intended once it is deployed. Specifically, it assesses the operational capability of five major groups of countermeasures for which FPS is contractually responsible: closed circuit television surveillance, contract security guards, intrusion detection systems, magnetometers, and x-ray machines. In some instances, contract guards are routinely evaluated to determine whether they are performing effectively. Performance includes the guards' knowledge of and compliance with relevant operations for their security post. Based on FPS testing results in fiscal year 2005, the baseline for this measure is 90-percent success, which is calculated as the number of countermeasures working and performing as intended divided by the number tested. According to FPS officials, FPS currently has about a 92-percent success rate for this measure. The long-term goal for this measure is 100-percent effectiveness. Related to facility protection, this output measure reflects the functionality of a program element, but not its effect.

Patrol and response, the third measure, assesses FPS's ability to respond to calls for service within certain time limit goals. The initial baseline for this measure was established in October 2005 and was about 17.5 minutes. This baseline represents an average response time for all of FPS's 11 regions, and is calculated using dispatch and arrival time information from FPS's online incident reporting system. The time parameters for data collection fell between FPS's core duty hours of 6:00 a.m. and 6:00 p.m. The goal for this measure is to reduce response times by 10 percent, although FPS noted that this goal could increase or decrease depending on staffing levels or deployments. At the time of this report, FPS noted that they have collected statistics on response times for this measure and are in the process of evaluating whether they have achieved their goal.

Finally, the facility security index—an outcome measure²⁹—calculates the overall effectiveness of FPS operations in meeting the performance goals of the three output measures described above (timely deployment of countermeasures, countermeasure functionality, and patrol and response

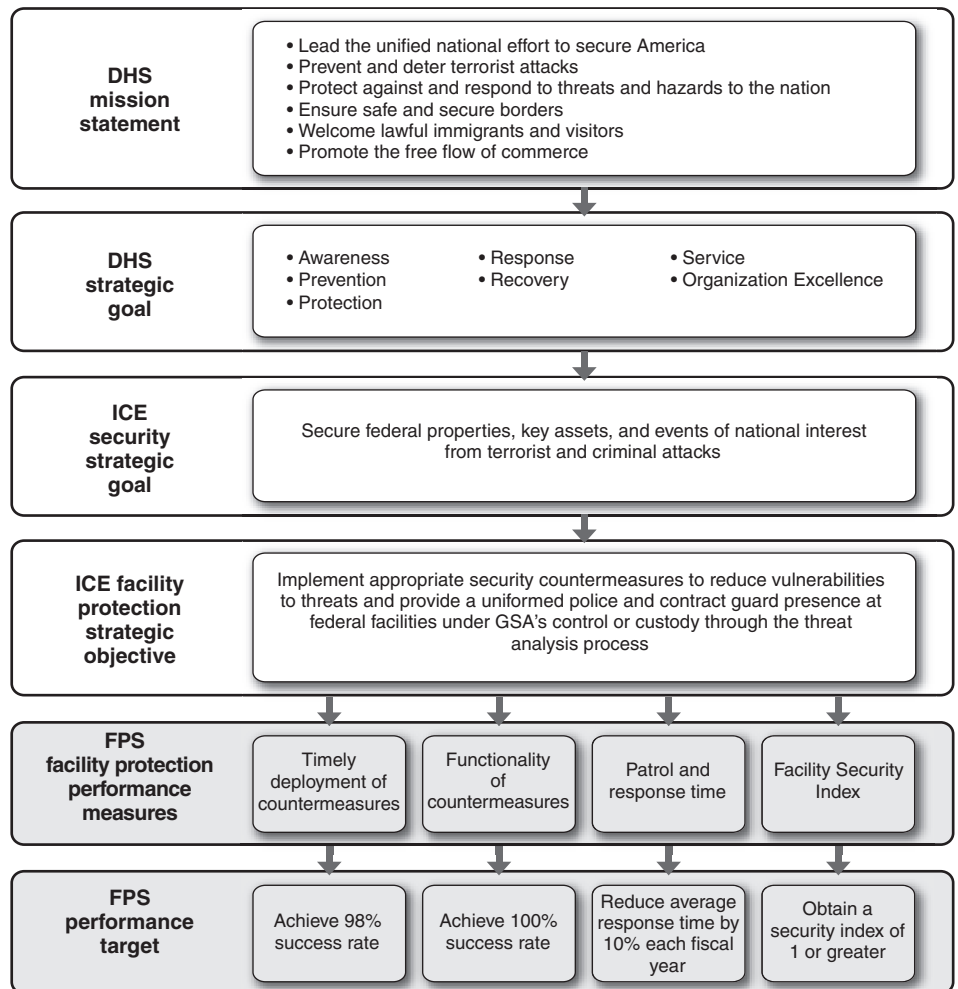
²⁹ Although FPS considers this an outcome measure, it is intended to reflect the composite level of performance of its three output measures.

time). An index score of 1 indicates that FPS has met its performance goals, a score of greater than 1 indicates that FPS has exceeded the goals, and a score of less than 1 indicates that it has not met the goals.

Taken together, these four FPS performance measures provide insight into activities designed to support FPS's efforts to prevent and respond to security and criminal incidents, including terrorist threats. In addition to assessing FPS's performance in fulfilling its facility protection responsibilities, the measures also serve as a baseline for making decisions about deploying existing resources or requesting additional resources. FPS officials told us that these measures are derived from strategic objectives established by DHS's Immigration and Customs Enforcement (ICE), of which FPS is a component. These objectives include implementing appropriate countermeasures to reduce vulnerabilities facing buildings under GSA's jurisdiction (see fig. 3). Aligning facility protection performance measures and targets with broader DHS and ICE mission, goals, and objectives helps hold employees accountable for security activity and allows them to observe how day-to-day security activities contribute to the broader mission, goals, and objectives. Similar to organizations outside the federal government, FPS provides its financial management staff with quarterly and annual reports that document the accomplishments for each measure in order to support planning and budgeting efforts included in DHS's Future Years Homeland Security Program document.³⁰

³⁰The Homeland Security Act requires that, beginning in fiscal year 2005, DHS prepare the Future Years Homeland Security Program document—a 5-year resource plan that outlines departmental priorities and the ramifications of program and budget decisions. See GAO, *Results Oriented Government: Improvements to DHS's Planning Process Would Enhance Usefulness and Accountability*, [GAO-05-300](#) (Washington, D.C.: Mar. 31, 2005).

Figure 3: Linkages between DHS Mission and FPS Performance Measures for Facility Protection



Source: GAO analysis of DHS data.

It is important to note that when FPS was a part of GSA, we reported on GSA's lack of performance goals and measures for its building security program. In June 1998, we testified that GSA had not established key program evaluation mechanisms for its building security program that could help determine how effective its security program has been in reducing or mitigating building security risks or in shaping new security

programs.³¹ At the time, we reported on features that would support program evaluation, including: (1) developing specific goals, outcomes, and performance indicators for the security program, such as reducing the number of unauthorized entries; (2) establishing and implementing systematic security program evaluations that provide feedback on how well the security program is achieving its objectives and contributing to GSA's strategic goals; and (3) ensuring that a reliable performance data information system is in place. While we found that GSA had established goals and measures for its security program both apart from and in connection with GPRA, we noted that these goals and measures were output oriented and did not address the outcomes or results the building security program was expected to achieve. Consequently, we recommended that GSA develop outcome-oriented goals and measures for its building security program. As previously noted, FPS has demonstrated some progress in moving beyond the use of output measures that monitor program activity in carrying out its responsibilities within the Department of Homeland Security (DHS).

In addition to FPS's performance measures for assessing the security of properties under GSA's control, GSA's Office of the Chief Architect also has a program for testing the physical security of GSA buildings. Under this program, GSA performs explosive testing of various window systems; identifies gaps in protective design and security technologies; and provides criteria and tools for blast resistant design, progressive collapse in new and existing facilities, and upgrading walls to reduce fragmentation and hazards resulting from an explosion, among other things. The program team is also developing a tool to identify gaps in security planning, ensure consistency with GSA policies and ISC's security design criteria, and provide a consistent foundation and methodology for making security design decisions.

Case Example: Interior's Bureau of Reclamation and National Park Service

One bureau within Interior—the Bureau of Reclamation (BOR)—has identified performance measures for its facility protection programs, while the National Park Service (Park Service) generates information that could be used to monitor the effectiveness of its physical security efforts. Each of Interior's eight bureaus independently manages the protection program for the facilities that fall under its respective purview, and each bureau has

³¹GAO, *General Services Administration: Many Building Security Upgrades Made But Problems Have Hindered Program Information*, [GAO/T-GGD-98-141](#) (Washington, D.C.: June 4, 1998).

developed broad security goals derived from the agency's overall mission.³² In general, Interior's program evaluation methods are based on GPRA and the Office of Management and Budget's (OMB) Program Assessment Rating Tool (PART).³³ Several of the bureaus have had their programs reviewed under the PART system, and some security performance measures were identified as part of this effort. Over time, Interior intends to have all of its law enforcement programs assessed under the PART system. However, an agency official from the Park Service reported difficulty in developing formal performance measures because GPRA is directed toward evaluating federal programs and does not provide guidance on developing goals and measures specifically for security activities.

Within Interior, BOR has an important role in protecting critical infrastructures because of its responsibilities related to dams. BOR is responsible for managing and protecting well-known assets such as Hoover Dam in Arizona and Nevada, which receives approximately 1 million paying visitors each year. In 2005, the security program administered by BOR was selected for review under the PART system. To demonstrate its progress in meeting the long-term goal of reducing security-related risks at its critical facilities, BOR developed several output and outcome performance measures, including (1) timely completion of risk assessments, (2) the cost per active background investigation, (3) the percentage of recommendations that have been implemented based on the results of risk assessments, (4) the number of updated regional threat assessments, and (5) changes in the risk ratings as countermeasures are implemented for an individual asset (see table 3). Although these measures were developed for the protection of dams and related facilities, they could be applied to building security because there is some similarity in the protection activities. In all but one instance, BOR had achieved or exceeded its performance target for each measure established for fiscal year 2005. According to OMB's PART assessment, BOR's facility protection program was rated moderately effective and its performance

³² However, to centrally manage Interior's security initiatives, the department established in 2002 a central coordination and oversight office for activities related to homeland security. This office—the Office of Law Enforcement and Security—has worked within Interior to identify assets that are likely targets, conduct risk assessments, and coordinate efforts by Interior's bureaus to enhance security at individual locations. See [GAO-05-790](#).

³³ OMB developed PART to support the integration of performance information and budgeting. OMB describes it as a diagnostic tool meant to provide a consistent approach to evaluating federal programs as part of the executive budget formulation process.

measures were described as creative and useful measures that will help monitor program accomplishments and efficiency.³⁴

Table 3: BOR's Performance Measures for Facility Protection

Type of measure	Performance measure	Purpose
Output	Timely completion of risk assessments	To compare actual completion dates with planned completion dates
Output	Cost per active background investigation file	To monitor the cost efficiency of the personnel security program, including processing of background investigations, issuance and verification of clearances, and case file maintenance
Output	Status of recommendations designed to mitigate risk	To indicate the percentage of recommended security enhancements that have been funded and implemented, and are operational
Output	Number of updated regional threat assessments	To assess the frequency with which assessments are conducted and help ensure that current threat intelligence is incorporated as part of risk assessments and risk-reduction strategies
Outcome	Change in risk ratings	To assess the risk-reduction benefits associated with implementing countermeasures at an individual asset

Source: GAO.

Note: GAO analysis of BOR data.

The Park Service is responsible for managing and protecting some of the nation's most treasured icons, including the Washington Monument, the Lincoln and Jefferson Memorials, and the Statue of Liberty. The Park Service manages more than 375 park units, covering more than 84 million acres, which provide recreational and educational opportunities and numerous other benefits to millions of visitors each year. From 2001 to 2005, park units averaged a total of about 274 million recreation visits per year. While a Park Service official stated that they did not have any formal performance measures for facility protection, we found that their risk management methodology provides useful feedback about the bureau's effectiveness in reducing or mitigating security risks for facilities under its jurisdiction. In June 2005, we reported that Interior had made significant progress in the risk assessment area, in large part due to its new National

³⁴ According to OMB, a moderately effective rating means that a program is well managed and has established ambitious goals. Programs with this rating likely need to improve their efficiency or address other problems in design or management to achieve better results. See www.expectmore.gov, which is a Web site that was developed by OMB and federal agencies to provide information on PART ratings.

Monuments and Icons Assessment Methodology (NM&I).³⁵ NM&I—a uniform risk assessment and ranking methodology—is specifically designed to quantify risk, identify needed countermeasures, and measure risk-reduction benefits at icon and monument assets. According to an Interior official, Interior’s Office of Law Enforcement and Security (OLES) developed NM&I to assist bureaus in quantifying risk levels and identifying needed security enhancements, initially at critical infrastructures and key assets, but eventually at all departmental facilities. The NM&I methodology has a consequence assessment phase and a risk assessment phase. First, during the consequence assessment phase, senior officials from the Park Service and OLES determine which icons are considered nationally significant.³⁶ Specific attack scenarios—such as chemical/biological, aircraft, or improvised explosive device—are used to evaluate security at each asset and score attack consequences.³⁷ During the risk assessment phase, a group of security professionals from the Park Service and OLES, assisted by the site security supervisor and the site manager, collectively determine the effectiveness of existing security systems using DHS guidelines. Using risk values calculated from this evaluation, OLES assigns asset risk ratings of high, medium, or low, and specific mitigation recommendations are formulated. As part of its annual review, OLES routinely monitors the security enhancements that have

³⁵See [GAO-05-790](#). Before the development of this approach, Interior did not have a uniform comprehensive risk management approach for national icons and monuments—most of which are highly visible and tend to have public access. It relied instead on the judgment of senior officials in determining where resources should be directed, and the risk assessments completed at individual sites were done by a number of external experts using different methodologies. In our June 2005 report, we recognized that Interior had made progress in addressing this concern but recommended that the agency link the results of its risk assessments and related risk rankings to its funding priorities and develop guiding principles for balancing security initiatives with its core mission. Regarding the recommendation to develop guiding principles, Interior officials told us that they have not made any progress on this effort, in large part because resources have been dedicated to meeting the requirements of a presidential directive that calls for governmentwide identification standards and processes for federal employees and contractors.

³⁶Interior officials said that they consider the following characteristics in determining which monuments and icons are nationally significant: (1) asset is widely recognized to represent the nation’s heritage, tradition, or values or is widely recognized to represent important national cultural, religious, historical or political significance; (2) asset’s primary purpose is to memorialize or represent some significant aspect of the nation’s heritage, tradition, or values, and to serve as a point of interest for visitors and educational activities; (3) if asset were successfully attacked, it would damage the American psyche and/or international confidence in the United States; and (4) asset is a monument, physical structure, or geographic site.

³⁷Consequence categories include casualties, economic impact, and length of disruption.

Case Example: USPS
Inspection Service

been implemented to reduce the risk rating designations. OLES has not had formal performance measures and targets for reducing risk ratings in the past. However, in April 2006, according to Interior officials, OLES developed and submitted for inclusion in the departmental strategic plan performance measures related to the reduction in the percentage of physical security vulnerabilities identified at departmental facilities. If adopted, such outcome measures could provide valuable feedback about the Park Service’s progress and overall effectiveness in protecting its physical assets.

The USPS Inspection Service utilizes an outcome-oriented performance measure to help ensure that it is progressing towards its strategic goal. USPS has over 38,000 facilities nationwide that collectively handle about 700 million pieces of mail every day, and the agency serves over 7.5 million customers daily in its post offices. Postal facilities are a compelling target for criminal and terrorist attacks, as evidenced by the anthrax attacks in 2001, which put at risk the integrity of the mail and the safety of USPS’s employees, customers, and assets. Within USPS, the Inspection Service—an investigative branch whose mission is to protect the nation’s mail system and its critical assets (i.e., employees, customers, and facilities)—established its first performance measure related to facility protection: the percentage of facilities that have high-risk ratings (see table 4).³⁸ This outcome measure allows the Inspection Service to monitor progress toward achieving its strategic goal of ensuring a safe, secure, and drug-free environment.

Table 4: Inspection Service’s Performance Measure for Facility Protection

Type of measure	Performance measure	Purpose
Outcome	Percentage of USPS facilities with high-risk ratings	To monitor the effectiveness of countermeasures through the percentage of USPS facilities that score more than 800 points

Source: GAO.

Note: GAO analysis of USPS data.

Specifically, this effort involves annual security surveys of facilities conducted by facility protection control officers, as well as periodic

³⁸In addition to the Inspection Service, USPS also has an Emergency Preparedness group that works in close conjunction with the Inspection Service to integrate emergency preparedness training and awareness from an operational perspective.

comprehensive reviews of larger core postal facilities performed by the Inspection Service. The data from these surveys and reviews are maintained in a database and used by the Inspection Service to tabulate a risk score based on USPS's Facility Risk Rating Model. Several data elements are considered to compute the composite risk score for a given facility, including:

- crime statistics;
- building characteristics (e.g., the absence or presence of customer parking, whether the facility is attached to an adjoining structure);
- location information (e.g., the number of federal buildings within a 1-mile radius of the post office);
- operational policies and procedures (e.g., the absence or presence of policies related to visitors, the timely completion of the facility security survey within the last 12 months); and
- countermeasures (e.g., the absence or presence of closed circuit television surveillance cameras).

Using these data elements, the maximum risk score that can be computed for a facility is 2,854 points. After each element at a particular facility is assigned a risk score, the system ranks the facilities according to the designated composite risk score. The scoring and ranking system is national and is applied to all USPS facilities, which allows officials to compare facilities across the country using standardized data to identify which buildings are at the highest risk level. Facilities with scores at or above the threshold score of 800 are considered to be high-risk.³⁹ The Inspection Service reassesses its facilities every 3 years or when a facility undergoes any major renovations or expansions. However, if a facility receives a high-risk score, the facility can be reassessed more often to help ensure that countermeasures are effective and that USPS has lowered the security risks. For example, if a facility received a high-risk score in fiscal

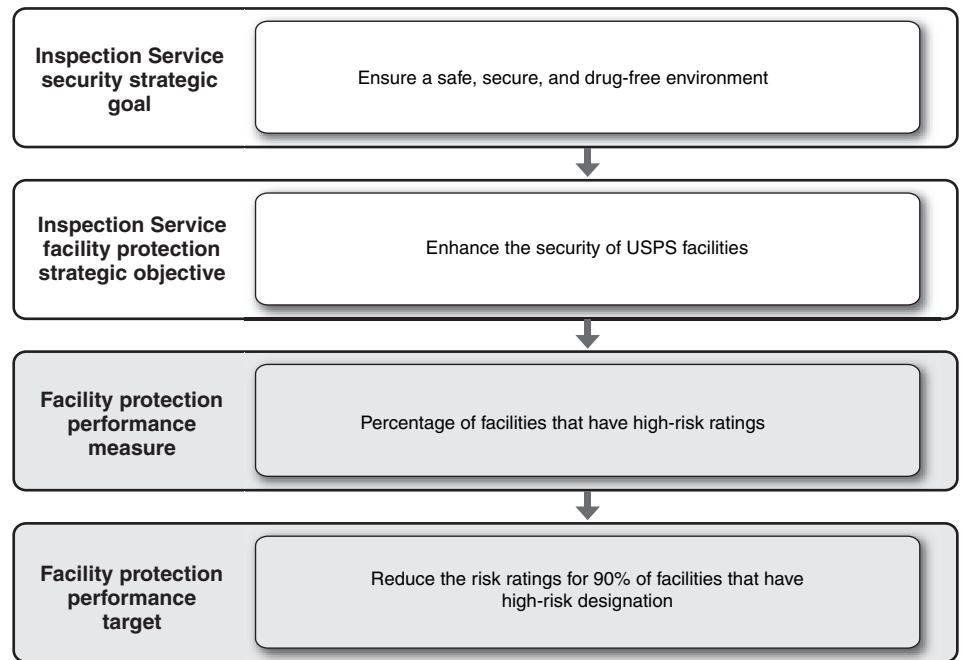
³⁹ Inspection Service officials told us that they chose 800 as the threshold score because they wanted to further review the security of the top 10 percent of the most vulnerable facilities. When this performance measure was implemented, the top 10 percent of most vulnerable facilities scored above 800. While this threshold remains the same today, the threshold score may decrease or increase over time due to implementation of countermeasures and changes in risk elements. To date, the Inspection Service has decided not to change the threshold score in order to keep the scoring methodology consistent.

year 2005, the Inspection Service will revisit that facility again in fiscal year 2006 to try to lower the risk score. The target is to reduce facility risk scores for 90 percent of the facilities that have a high-risk designation. At the time of our review, USPS was successful in meeting its performance target, according to Inspection Service officials.

The Inspection Service's outcome performance measure, outlined above, is closely aligned with its strategic goal—to ensure a safe, secure, and drug-free environment—and with its strategic objective—to enhance the security of USPS facilities. Linking their performance measures and targets with their strategic goals and objectives in this way provides managers and staff in the Inspection Service with a roadmap that shows how their day-to-day activities contribute to achieving broader Inspection Service goals (see fig. 4). Inspection Service officials told us that they designed their security-related strategic goal and objective to support USPS's broader strategic goal of improving services, which includes activities that protect mail, employees, and customers in order to improve services.⁴⁰

⁴⁰In its Strategic Transformation Plan 2006-2010, USPS has identified four strategic goals: (1) generate revenue; (2) reduce costs; (3) achieve results with a customer-focused, performance-based culture; and (4) improve service.

Figure 4: Linkages between USPS Inspection Service Strategic Goals and Performance Measure for Facility Protection



Source: GAO analysis of USPS data.

Case Example: Department of Veterans Affairs

Although it does not use security performance measures, VA collects data that could be used to assess the effectiveness of the agency's facility protection program. VA manages a large health system for veterans that now includes 154 medical centers, 875 ambulatory care and community-based outpatient clinics, and 136 nursing homes. In 2005, more than 5 million people received care in VA health care facilities, and VA's outpatient clinics registered nearly 58 million visits. VA also operates 61 major veterans' benefits facilities, including 57 regional offices, 3 records centers, and headquarters.⁴¹ While VA officials noted the absence of performance measures for facility protection, we found that the Veterans Health Administration and the Veterans Benefit Administration rely on

⁴¹VA officials noted that the majority of the space occupied by VA's Veterans Benefit Administration is in GSA-held buildings. As such, FPS is responsible for security at these facilities.

physical security assessments to inform risk-management and resource-allocation decisions, just as other federal agencies and nonfederal entities do. The phases of the physical security assessment include defining the criticality of VA facilities, identifying and analyzing the vulnerabilities of VA's critical facilities, and identifying appropriate countermeasures. VA determines vulnerability based on factors such as facility population, building characteristics (e.g., the number of floors in the facility), and the presence or absence of armed officers and surveillance cameras. VA's assessment includes a procedure for scoring and prioritizing identified vulnerabilities at each assessed site. The objective of the security assessment is to identify shortcomings in the physical security of functional areas within critical facilities and to estimate the cost of mitigating the risk of disruption or termination of the facility's ability to provide services to veterans. For example, they assess the vulnerability of a facility's air system to a criminal attack. For each assessed functional area, a composite score and corresponding risk rating is assigned. The risk-rating system is based on a color-coded "traffic light" scheme to designate low-, medium-, and high-risk functional areas. The results from the security assessment—in particular, the risk-rating designation—are used to develop recommendations to mitigate the security risk and to prioritize and justify resource-allocation decisions. VA officials said that they had conducted full assessments at 18 critical facilities and revisited these facilities a year later to determine progress since the assessment. At the time, approximately 16 percent of recommended mitigation items had been completed, were in progress, or had been planned for. VA officials said they are finalizing a database and software that would facilitate the tracking of facilities' responses to assessment recommendations. The officials said that they expect to roll out the database and software within a few months.

Besides conducting security assessments, organizations can mitigate risk by testing their facility protection countermeasures. Like FPS, VA conducts inspections and tests to evaluate compliance with security policies and procedures and to help ensure that adequate levels of protection are employed. In some instances, such as in the VA headquarters building, inspections can include simulated attempts to gain unauthorized access to a building or to smuggle fake weapons into a

building.⁴² For example, within VA, scenario-based tests that are derived from emerging security threats are commonly used to assess police officers' knowledge of, and compliance with, policies and procedures and to evaluate preparedness in the event of an attack. Earlier in this report, we noted that FPS has developed a performance measure using similar tests in order to assess the effectiveness of security countermeasures, such as contract security guards, in mitigating risk. In addition, both VA and FPS conduct biannual inspections of compliance with standards and policies, including for physical security.

Such measurable activity could enable the measurement of program outcomes, including changes in the number of unauthorized building entries or the number of weapons and other prohibited items detected as part of facility intrusion tests. Although VA officials told us they had not developed performance measures, we believe they have valuable data that can be used to measure the overall effectiveness of the agency's facility protection program. For VA, security assessments and testing activity provide useful feedback on how well security measures have operated and whether they continue to be appropriate for the future. Further, these evaluations could form the basis for overall evaluations of VA's building security program and could provide data for performance measurement initiatives.

Federal Guidance for Developing and Using Performance Measures Exists for IT Security, but Not for Physical Security

While performance measures have been used to monitor many federal programs, little has been done to apply performance measurement to physical security programs—a complex and challenging undertaking, since outcomes may not be quickly achieved or readily observable. Although we found that physical security performance measurement is a challenge for many organizations in the public and private sector, we found that the information technology (IT) security area has performance measurement initiatives under way. Similar to facility protection, IT security has been a considerable concern in large part because computer systems are vital to many of our nation's critical operations and infrastructure. The dependency on these systems prompted a number of congressional actions, including various mandates for agencies to

⁴²VA officials noted that most Veterans Health Administration buildings are designed for maximum public access and therefore do not have magnetometers or metal detectors, so such tests are not conducted in those facilities. In addition, many Veterans Benefit Administration facilities are in GSA buildings, so FPS is responsible for providing security and conducting related tests.

implement security controls to protect information systems within the federal government. In compliance with these federal requirements, agencies must demonstrate their progress in meeting requisite information security requirements and report on their actual level of performance based on the results of annual program reviews.

In its role as a leader on technology issues, the National Institute of Standards and Technology (NIST), a subagency within the Department of Commerce, issued a report in 2003—*Security Metrics Guide for Information Technology Systems*—to provide guidance on how an organization can use performance measures to determine the adequacy of in-place security controls, policies, and procedures intended to mitigate security risks.⁴³ More specifically, the report provides an approach that helps managers decide where to invest additional security protection resources or how to identify and evaluate controls that are not effective. The guidance is the culmination of several efforts to identify a suitable method for measuring security and supplemented ongoing initiatives by OMB to help agencies develop workable measures of job and program performance that would hold federal employees accountable for their IT security responsibilities. In addition to providing practical examples of security performance measures that can be readily used or modified to meet agency-specific needs, the report provides a detailed description of how performance measurement is being approached in the IT security area and addresses the following areas: (1) the roles and responsibilities of agency staff at all levels, (2) the benefits of using performance measures, and (3) an overview of the performance measures development and implementation process.

The NIST report advocates the use of measurable performance measures based on IT security performance goals and objectives. In turn, the report describes performance measures as tools designed to facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data. NIST describes three types of performance measures—implementation, efficiency and effectiveness, and impact—that can be used to measure progress (see table 5). Although NIST uses different terminology to describe the three types of performance measures, they are similar to the output and outcome measures that we have advocated for use in

⁴³National Institute of Standards and Technology, *Security Metrics Guide for Information Technology Systems*, NIST Special Publication 800-55 (July 2003).

monitoring and reporting program accomplishments. The NIST report cautions that the type of performance measures that can realistically be obtained and used for performance improvement depends on the maturity of the security program. According to NIST, in the early stages of establishing a security program, the focus tends to be on developing security policies and procedures, and beginning to ensure that security controls are implemented. In such an environment, an appropriate performance measure would be one that focuses on implementation, such as the percentage of information systems with approved security plans. In contrast, a more mature security program may evolve to measure the efficiency and effectiveness of security controls and the impact of these controls on the organization's mission. In such cases, the performance measures may concentrate on the evidence and results of testing.

Table 5: Types of Information Technology Security Performance Measures Described by NIST

Type of measure	Performance measure	Purpose
Implementation	Percentage of systems with approved security plans and the percentage of systems with password policies configured as required	Assess the extent to which security plans and password policies have been documented and implemented to support the security program
Efficiency and effectiveness	Percentage of crackable passwords within a predefined time threshold	Evaluate the results of security controls that have been implemented; validate whether security controls, as described in the security plan, are effective in protecting the organization's assets
Impact	Quantify incidents by type (e.g., root compromise, password compromise, malicious code, denial of service) and correlate incident data with the percentage of trained users and system administrators	Measure the impact of training on security

Source: NIST.

The guidance goes beyond extolling the virtues of using performance measures and illustrates the place of IT security within a larger organizational context, provides a roadmap for how to develop and implement a performance measurement program, and includes practical examples of performance measures. According to NIST, the performance measures that are ultimately selected can be useful not only for measuring performance, identifying causes of unsatisfactory measurements, and pinpointing improvement areas, but also for facilitating continuous policy implementation, effecting security policy changes, and redefining goals and objectives. NIST notes that successful implementation of a security performance measurement program can also assist agencies in meeting

OMB's annual requirements to report the status of agency IT security programs. In addition to providing examples of performance measures, some of which are required by OMB, the report also includes a standardized template that describes the various data elements that should be documented (see fig. 5). The data elements include:

- *Performance goal*: States the desired results of implementing security control objectives that are measured by the metric.
- *Performance objective*: States the actions that are required to accomplish the performance goal.
- *Metric*: Defines the metric by describing the quantitative measurements it provides.
- *Purpose*: Describes the overall functionality obtained by collecting the metric; includes whether a metric will be used for internal performance measurement or for external reporting, what insights are hoped to be gained from the metric, and whether regulatory or legal lessons exist for collecting a specific metric if applicable.
- *Implementation evidence*: Includes indirect indicators that validate that the activity is being performed and causation factors that may point to the causes of unsatisfactory results for a specific metric.
- *Frequency*: Establishes time periods for collecting data that is used for measuring changes over time.
- *Formula*: Describes the calculation to be performed that results in a numeric expression of the metric.
- *Data source*: Identifies the location of the data to be used in calculating the metric (e.g., databases, tracking tools, organizations, or specific roles within the organization that can provide required information).
- *Indicators*: Provide information about the meaning of the metric and its performance trend; state the performance target and indicate what trends would be considered positive in relation to the performance target.

The NIST report notes that the universe of possible performance measures, based on policies and procedures in place in the organization, will be quite substantial and that the final performance measurement set selected for initial implementation should relate to high-priority areas, use data that can be realistically obtained, and measure processes that already

exist and are relatively stable. The guidance further states that performance measures can be developed and selected using a phased approach. This approach identifies short-, mid-, and long-term measures where the time frame in which these measures are implemented depends on a combination of system-level effectiveness, performance measure priority, data availability, and process stability. The NIST report also notes that, once applicable performance measures have been identified, they should be documented using a standardized template (see figure 5). Standardizing the reporting process is particularly useful in cases where the reporting process within an organization is inconsistent. Such practices, among others, can help ensure the success of a performance measurement program.

Figure 5: Sample Standardized Performance Measurement Data Form

A.1 Risk Management	
Critical Element	1.1 Is risk periodically assessed?
Subordinate Question	1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities or other conditions change?
Metric	Percentage of systems that had formal risk assessments performed and documented
Purpose	To quantify the number of risk assessments completed in relation to the organization's requirements.
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? Yes No 2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____ 3. Of the systems in your current inventory, how many systems have had risk assessments performed and documented in the following time frames? (Select the nearest time frame for each system; do not count the same system in more than one time frame.) Within past 12 months_____ Within past 2 years_____ Within past 3 years_____ 4. For any system that underwent a risk assessment, list the number of systems after the reason(s) that apply: Scheduled risk assessment_____ Major change in system environment_____ Major change in facilities_____ Change in other conditions (specify) _____ 5. For any system that has not undergone a risk assessment in the past 3 years, list the number of systems after the reason(s) that apply: No policy_____ No resources_____ System tier level does not require _____ System previously not defined_____ New system _____ Other (specify) _____
Frequency	Semiannually, annually
Formula	At agency level: Sum of risk assessments on file for each time frame (Question 3) / IT systems in inventory (inventory database) (Question 2) ¹
Data Source	Inventory of IT systems that includes all major applications and general support systems; risk assessment repository
Indicators	This metric computes the percentage of systems that have undergone risk assessments over the last three years (which is normally the required maximum time interval for conducting risk assessments). To establish the distribution of time for risk assessment completion, the number of systems listed for each time frame is computed. The total within three years should equal 100 percent of all required systems. Systems that are not receiving regular risk assessments are likely to be exposed to threats. Question 4 is used to validate the reasons for conducting risk assessments and to ensure that all systems are accounted. Question 5 is included to determine the reason risk assessments were not performed. Defining the cause will direct management attention to the appropriate corrective actions. By documenting and tracking these factors, changes can be made to improve performance by updating the security policy, directing resources, or ensuring that new systems are assessed for risk as required.
Comments: A number of additional metrics may be created to ascertain the number of systems that have undergone risk assessments after a major change, a number of systems that have undergone risk assessments during the last year after a major change, and others. This information can be tracked separately to ensure that this requirement is met and that system changes are monitored and responded to appropriately in a timely manner. A system may have had a risk assessment within the past two years, but if a major change has occurred since then, an additional risk assessment is required to ensure that information about the system's vulnerabilities and exposure to risk is updated and the risk managed.	
¹For metrics that ask for a percentage the result of the formula should be multiplied by a hundred to produce a percentage value.	

Source: NIST.

Federal Agencies Have
Received Minimal Guidance on
Using Performance
Measurement for Facility
Protection Programs

We have previously reported that, at the agencywide level, agencies face obstacles in developing meaningful, outcome-oriented performance goals and in collecting data that can be used to assess the true impact of facility protection efforts. GPRA emphasizes measuring the results of products and services delivered by a federal program (i.e., outcomes). For programs that have readily observable results or outcomes, performance measurement may provide sufficient information to evaluate the effectiveness of facility protection efforts. Yet in some programs, such as facility protection, outcomes are not quickly achieved or readily observable, or their relationship to the program is often not clearly defined. In such cases, more in-depth program evaluations, in addition to performance measurement, may be needed to examine the extent to which a program is achieving its objectives.

While federal agencies have made some progress developing performance measures for facility protection, we noted that the emphasis is on using output measures that monitor program activity rather than outcome measures that assess the overall impact of program activity. This lack of outcome measures leaves agencies with insufficient information to determine whether security activities are effective and to evaluate whether the benefits of security investments justify their costs. We have previously reported that various security program outputs—such as conducting patrols—may have contributed to improved security, but that using them as performance measures may not systematically target areas of higher risk and may not result in the most effective use of resources, because these measures are not pointed toward outcomes. Such output measures do not provide an indication of what these activities are accomplishing. By contrast, outcome measures that are clearly tied to results would indicate the extent of progress made and help identify the security gaps that still remain.⁴⁴ Without more information on security program outcomes, agencies do not know the extent to which security enhancements have improved security or reduced federal facilities' vulnerability to acts of terrorism or other forms of violence. In addition, there is some inconsistency in the types of activities that are being monitored and used as indicators of an agency's progress in fulfilling its facility protection responsibilities. If agencies use inconsistent approaches to performance measurement, decision makers could be at risk of having incomparable performance information to determine funding priorities within and across agencies.

⁴⁴[GAO-06-91](#).

Echoing what organizations outside the U.S. federal government told us, some agency security officials said it was challenging to measure the impact that various approaches have on actually improving security. Some agency officials also noted that resources for performance measurement initiatives were scarce. Additionally, the availability of information needed for applying performance measurement to facility protection is somewhat limited. More generally, with the exception of DHS, the agencies that we reviewed do not view security as their primary mission, and some agencies are faced with competing demands for limited resources to accomplish broader agency goals. In such an environment, security must be integrated using scarce resources.

In spite of the inherent difficulty in measuring facility protection performance, and the considerable emphasis on doing so, agencies have minimal guidance on how to accomplish this. There is, however, broad guidance for the protection of critical infrastructures, which includes government facilities. Using a risk-based approach, the Draft National Infrastructure Protection Plan (NIPP) was developed to provide an integrated, comprehensive approach to addressing physical, cyber, and human threats and vulnerabilities.⁴⁵ As part of the NIPP, DHS officials have provided guidance and collected information on core performance measures—which are common measures that can be broadly applied to all protection programs for critical infrastructures and key assets. These measures are mostly process/input and output oriented, and DHS officials noted that they hope to develop outcome measures as the program matures. The NIPP, however, does not provide or collect information on specific performance measures related to the protection of federal facilities. Rather, it notes that FPS—the agency assigned responsibility for implementing the NIPP framework and guidance in the government facilities sector—will develop such performance measures. Separately, OMB issued a memorandum in June 2004 that reported it was working with agencies on initiatives related to physical security reporting requirements noted in Homeland Security Presidential Directive Number 7 (HSPD-7).⁴⁶ The memorandum instructed each agency to disclose the

⁴⁵DHS released the first Draft NIPP for public comment in November 2005. In January 2006, DHS released a revised Draft NIPP that incorporated some of the comments it had already received.

⁴⁶As mentioned earlier, HSPD-7 establishes a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructures and key assets so that they can be protected from terrorist attacks.

performance measures it had designed and implemented to measure outputs and outcomes. However, OMB did not provide specific guidance or standards and instead directed agencies to use DHS guidance—related to the NIPP—that does not specify measures for facility protection.

By contrast, the IT security performance measurement guidance issued by NIST includes information on: (1) clearly defining roles and responsibilities for relevant stakeholders; (2) establishing security goals and objectives; (3) identifying and implementing performance measures and performance targets; and (4) using measures that are unique to IT security to assess the impact of IT security efforts. One security official from the gaming industry said that IT security performance was somewhat easier to evaluate than physical security performance because it is possible to directly monitor the number of attempted IT security breaches. A foreign government agency we interviewed is farther along in developing standards and performance measures for IT security than for physical security. In general, IT security approaches are slightly more standardized than physical security because the field is newer than physical security and because organizations had to work together to prepare for possible complications in the year 2000 (Y2K). Despite such differences between IT and physical security performance measurement, some of the performance measurement guidance could be applicable to physical security situations.

ISC is a body that addresses governmentwide security policy issues and, like NIST, is well positioned to develop guidance and promote performance measurement. Executive Order 12977 calls for ISC to play an oversight role in implementing appropriate security measures in federal facilities and taking actions that would enhance the quality and effectiveness of security in federal facilities. As we reported in November 2004, ISC has already made progress in coordinating the federal government's facility protection efforts through activities such as developing security policies and standards for leased space, improving information sharing, and coordinating the development of a security database of all federal facilities.⁴⁷ The ISC Chair told us that he supports the use of performance measurement as a means of strengthening federal facility protection efforts.

⁴⁷See [GAO-05-49](#).

Conclusions

Given their competing priorities and limited security resources, U.S. federal agencies could benefit from specific performance measurement guidance and standards for facility protection to help them address the challenges they face and help ensure that their physical security efforts are achieving the desired results. While some of these agencies have implemented performance measures to monitor their security programs' outputs, fewer have developed outcome measures to assess the extent to which security enhancements have improved security or reduced their facilities' vulnerability to acts of terrorism or other forms of violence. Without a means of comparing security effectiveness across facilities, particularly program outcomes, the U.S. government is open to the risk of either spending more money for less effective physical security or investing in the wrong areas. The output measures that federal agencies have developed provide an indication of what their security activities are accomplishing but do not indicate the extent of progress made or help identify the security gaps that still remain, as outcome measures would. Fundamentally, performance measurement helps ensure accountability, since it enables decision makers to isolate certain activities that are hindering an agency's ability to achieve its strategic goals. Performance measurement can also be used to prioritize security needs and justify investment decisions so that an agency can maximize available resources. Over time, a thorough performance measurement approach could allow the federal government to manage the risks to federal facilities both within and across agencies. Recognizing the unique nature of U.S. federal agencies' missions, some uniformity in measuring performance in facility protection efforts could facilitate comparisons across agencies.

Organizations outside of the U.S. government—including private-sector entities as well as state, local, and foreign government agencies—have developed and are using performance measures for facility protection, and their knowledge and experience could be helpful to U.S. federal agencies in developing and refining their own performance measures. Likewise, because the application of performance measures to facility protection can be challenging, many nonfederal organizations are looking to U.S. government agencies for assistance and leadership. Some U.S. federal agencies are already collecting data that could be used for measuring security performance, and they currently have guidance for measuring information technology security, but not physical security. The U.S. federal government has provided guidance and collected information on a set of common measures that can be broadly applied to all protection programs for critical infrastructures and key assets, and agencies will be required to report on additional security performance measures that are sector-specific. With regard to federal facilities, the ISC, in serving as the

central coordinator for U.S. agencies' federal facility protection efforts, is well positioned to develop and promote performance measurement guidance and standards for physical security, and could look to information technology security as a model to follow. In turn, it could draw from examples of performance measurement we identified in the private sector and foreign government agencies. Federal agencies could subsequently follow the guidance and standards to evaluate their actions, identify lessons learned, and develop strategies for overcoming any challenges in developing and using performance measures for facility protection. Because of the ever-changing nature of security threats and new security technologies and countermeasures, such guidance and standards would need to be periodically reviewed and updated. The development of guidance and standards for facility protection could help ensure uniform application of performance measurement so that the U.S. federal government, particularly its largest real-property-holding agencies, would be accountable for its facility protection programs and would be able to demonstrate that security investments are producing a return, both within and across agencies, in terms of better-protected facilities.

Recommendations for Executive Action

To ensure that useful information is available for making decisions about the allocation of resources for, and the effectiveness of investments in, the protection of federal facilities, we recommend that the Secretary of Homeland Security direct the Chair of ISC to do the following:

- as part of ISC's efforts to support DHS in developing sector-specific performance measures for the security of federal government facilities, establish guidance and standards, with input from ISC member agencies, for measuring performance in facility protection—with a particular focus on developing outcome measures;
- communicate the established guidance and standards to the relevant federal agencies; and
- ensure that the guidance and standards are regularly reviewed and updated.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS, GSA, USPS, VA, and Interior for their official review and comment. DHS concurred with the report's overall findings and recommendations. DHS comments are contained in appendix III. USPS and VA concurred with the report's findings. In addition, DHS and USPS provided separate technical comments, which we

incorporated into the final report where appropriate. GSA notified us that they had no comments on this report.

Interior, while generally agreeing with the report's findings, suggested that an agency-by-agency assessment of each federal agency's facility vulnerabilities would be more effective than a cross-agency facility protection performance measure. We agree that identifying and monitoring vulnerabilities is important, but believe that it is also important for decision makers to have comparable information about the relative security performance of facilities within an agency as well as across the federal government. Interior also expressed concern that a more public viewing of agency facility protection performance could reveal weaknesses or vulnerabilities that could be exploited. We agree that this could be a concern but leave the development of guidelines for using and protecting this information to ISC and its member agencies. Interior also provided technical comments, which we incorporated. Comments from Interior and our evaluation can be found in appendix IV.

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 the Interior, Homeland Security, and 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. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

Sincerely yours,

A handwritten signature in black ink, appearing to read 'M. Goldstein', with a long, sweeping horizontal line extending to the right.

Mark L. Goldstein
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our report were (1) to identify examples of performance measures for facility protection being used by selected organizations outside of the federal government—including private-sector entities, state and local governments, and foreign governments; and (2) to determine the status of U.S. federal agencies' efforts to develop and use performance measures as part of their facility protection programs.

To identify examples of performance measures for facility protection being used by selected organizations outside the federal government, we interviewed representatives from the private sector, U.S. state and local governments, and foreign governments. With respect to the private sector, we asked a number of umbrella organizations to identify industries that are likely to utilize performance measures for facility protection and known leaders in the security performance measurement area. These umbrella organizations included ASIS International, Real Estate Roundtable, Financial Services Roundtable, Financial Services Information Sharing and Analysis Committee, International Facility Management Association, and National Association of Industrial and Office Properties. GAO staff also attended the annual ASIS International Conference in 2005. Some of these entities stated that the gaming and finance industries would be the most appropriate to review, since these industries have invested significantly in the quality of their security efforts. As a result, we interviewed officials from four gaming entities and five major financial services organizations. To maintain the organizations' security and the confidentiality of proprietary information, we do not identify specific organizations in this report.

For the gaming industry, a member of the Real Estate Roundtable provided a contact who was known to be active in physical security testing and performance measurement. This individual then arranged a joint interview for us with a number of gaming entities. Some of the representatives present at the interview were also members of the Las Vegas Security Chiefs Association or ASIS International Gaming and Wagering Council. The five financial services organizations we interviewed were selected because they (1) were considered to be leaders in their industry; (2) were recommended by others within the industry; (3) were members of ASIS International, the largest organization supporting security professionals; or (4) have had prior security concerns related to threats of terrorism.

To determine if U.S. state and local governments have developed performance measures for facility protection, we attempted to contact 10 state and 10 local governments. For state governments, we selected the 10

states receiving the most funding from the Department of Homeland Security's (DHS) State Homeland Security Program grant in fiscal year 2005. For local governments, we selected the 10 local governments/urban areas receiving the most funding from DHS's Urban Areas Security Initiative grant in fiscal year 2005.¹ Of the 20 state and local governments we attempted to contact, we were able to obtain information from officials from 17 of them. While all 17 of these state and local governments were engaged in facility protection efforts, only a few had developed performance measures to evaluate the effectiveness of these efforts. Table 6 shows a listing of these state and local governments. The agencies we approached within each of the state and local governments were often, but not always, the agencies responsible for real property or policing/security. Some of the state and local governments we attempted to contact were also identified by the Government Accounting Standards Board as having performance measurement initiatives on a variety of their organizations, departments, and projects.

¹The State Homeland Security Program and Urban Areas Security Initiative grants can be applied to a number of homeland security efforts, including facility protection. See U.S. Department of Homeland Security, *Fiscal Year 2005 Homeland Security Grant Program, Program Guidelines and Application Kit*.

Table 6: U.S. State and Local Governments Contacted

Organization	Location
U.S. state governments	California
	Florida
	Georgia
	Illinois
	Michigan
	New Jersey
	New York
	Ohio
	Pennsylvania
	Texas
U.S. local governments	Boston, Mass.
	Detroit, Mich.
	Washington, D.C. ^a
	Los Angeles, Calif.
	New York, N.Y.
	Philadelphia, Pa.
	San Francisco, Calif.

Source: GAO.

^aFor the purposes of this report, Washington, D.C., was treated as a local government.

For our work with foreign governments, we conducted international site visits in three foreign countries—Australia, Canada, and the United Kingdom—where we interviewed a number of government agencies and organizations about their use of performance measures for facility protection. (Table 7 shows a listing of each of these agencies.) We selected these three countries for site visits because they are known to have experience with threats of terrorism and because they have been identified by the Government Accounting Standards Board as having performance measurement initiatives, not necessarily for facility protection but for government initiatives in general. We also spoke with representatives from a number of other foreign governments. While these other governments have facility protection efforts in place, they said they did not use performance measures to assess the effectiveness of these efforts. Furthermore, officials from some of these countries told us that they look to the United States for guidance on a number of issues relating to facility protection, including how to measure effectiveness. For such reasons, these countries were not highlighted in this report.

Table 7: Foreign Government Agencies and Organizations Visited

Location	Organization
Australia	Airservices Australia
	Attorney-General's Department
	Commonwealth Scientific and Industrial Research Organization
	Customs Service
	Department of Defence
	Department of Foreign Affairs and Trade
	Federal Police
	National Audit Office
	Taxation Office
Canada	Bank of Canada
	Corps of Commissionaires
	Department of National Defence
	National Gallery
	Office of Auditor General
	Public Works and Government Services Canada
	Royal Canadian Mounted Police
	Treasury Board
United Kingdom	Cabinet Office
	Department for Transport
	Foreign and Commonwealth Office
	Home Office
	National Infrastructure Security Coordination Centre, Security Service
	National Security Advice Centre, Security Service
	Office for Civil Nuclear Security

Source: GAO.

In addition to interviewing officials from the nonfederal entities identified above, we reviewed relevant documentation obtained from these organizations, previous GAO reports, and performance measurement and facility protection literature from ASIS International and other sources.

For the second objective—to determine the status of U.S. federal agencies’ efforts to develop and use performance measures as part of their facility protection programs—we interviewed selected officials from the major civilian real property holding agencies. These agencies include the General Services Administration (GSA), the United States Postal Service (USPS), the Department of Veterans Affairs (VA), and the Department of Interior

(Interior). GSA acknowledged the need to measure the performance of facility protection efforts; however, for most facility protection issues, they defer to the Federal Protective Service (FPS) within DHS. Because FPS is responsible for protecting all GSA buildings, we also interviewed officials from FPS. For each of the selected federal agencies, we reviewed agency strategic and performance plans, security goals, performance reports, and other relevant documentation provided to us. We also interviewed the Executive Director of the Interagency Security Committee (ISC)—a DHS-led committee that is tasked with coordinating federal agencies' facility protection efforts. Finally, we reviewed a number of national strategies and presidential directives; previous GAO reports; and relevant reports by the Office of Management and Budget, the Congressional Budget Office, the Congressional Research Service, and other government entities. We also reviewed laws and authorities related to facility protection.

It is important to note that the private-sector entities, U.S. state and local governments, and foreign governments selected for our review are not representative of the universe of such organizations. Furthermore, GAO has not evaluated the robustness and quality of the performance measures cited in this report. Rather, these measures are simply a compilation of what we have gathered from the nonfederal and federal entities we have interviewed. Additionally, the performance measures identified in this report may not include all performance measures relating to the protection of federal facilities. We used our judgment to classify the performance measures into process/input, output, and outcome measures according to our definitions, but these performance measures could be classified differently depending on the performance measurement goals or objectives used by an organization.

Also, ISC has identified GAO as an associate member, which includes the ability to serve on ISC subcommittees. No GAO staff member, however, 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.

Officials from nonfederal and federal entities provided much of the information used in this report. In most cases where officials provided their views as representatives of their organizations, we corroborated the information with other officials or with documentation provided to us. We

requested official comments on this report from DHS, GSA, USPS, VA, and Interior. Furthermore, when we used examples from the private sector, state and local governments, foreign governments, and the National Institute of Standards and Technology (NIST), we provided the respective entity an opportunity to review relevant portions of the report and offer comments, thus ensuring the validity of our reporting. We conducted site visits and interviews from July 2005 through January 2006. We conducted our work from May 2005 through April 2006 in accordance with generally accepted government auditing standards.

Appendix II: Examples of Performance Measures Used by Selected Organizations outside of the Federal Government

The performance measures below were provided by the selected organizations we interviewed outside of the federal government. We did not evaluate the quality of the performance measures, and we used our judgment to classify them according to the following definitions of performance measures:

- Output measures focus on the quantity of direct products and services a program delivers and the characteristics of those outputs, including efficiency, cost-effectiveness, timeliness, quality, and customer service.
- Outcome measures provide information on the results of the direct products and services a program has delivered.
- Process/input measures address the type or level of program activities an organization conducts and the resources used by the program.

The performance measures could be classified differently depending on the performance measurement goals or objectives used by an organization.

Output
Number of risk assessments performed New security projects • Security checklist completed during planning stages • Security officials consulted Number of security requests received • Security report requests • New access badge requests • Requests for changes to existing badges Security clearance • Number of background screenings completed • Average time to process background screenings • Average number of days to process security clearances • Number of overdue security clearances by more than 4 weeks • Cost per security clearance • Percentage of officers/contractors who hold sufficient level of security clearance when compared to their duties Alarm systems • Responded to and cleared • Alarms with unique responses (i.e., alarms requiring guards to respond in person) • Failed to arm

Appendix II: Examples of Performance Measures Used by Selected Organizations outside of the Federal Government

Number of police incidents/reports filed Number of threats • Against employees • Against facilities Security incident reaction/response • Number of avoidable incidents detected • All significant investigations completed within 45 days Compliance with security policies and standards • Number of exceptions reviewed • Number of significant policy breaches • Surveillance and communication systems are compliant with standards • Entry/access control systems are compliant with standards • Security staff are fulfilling their contract obligations Customer/client satisfaction • Staffing—training, professional appearance, professional behavior, turnover rate, supervision • Security reporting—accuracy, timeliness, use of correct forms • Management—responsiveness, understanding of issues, availability, number of personal contacts Timely delivery of security alerts and briefings Percentage of alarms responded to within 20 minutes during nonpublic service hours Increased attendance at training courses for security officers Number of new employees, contractors, and consultants who have not attended a security awareness session within 4 weeks of receiving their identification pass Percentage of security guards in compliance with licensing standards within a 7-day period All scheduled audit and compliance reports completed in 14 days
Outcome
Change in the total number of security-related incidents • Accident • Assault • Burglary • Organization assets • Personal assets • Drugs/Alcohol

Appendix II: Examples of Performance Measures Used by Selected Organizations outside of the Federal Government

• Extortion • Fire • Fraud Referral • Harassment • Larceny/Theft • Malicious damage • Public disorder • Robbery • Suspicious activity • Terrorism • Vandalism • Workplace violence Evidence of damage to building and facilities Evidence of harm to staff or tenants Change in risk rating resulting from countermeasures deployed Security policies and practices receive favorable comment from security audit program Agency stakeholders view agency as a safe custodian of allocated resources and assets
Process/Input
Number of facilities being protected (including types and locations) Number of security staff Number of security guards/security escorts Personal security arrangements for after-hours entry/access Perimeter security • Assessment of entry/exit points • Serviceability of perimeter security equipment (locks, door frames, security signs) • Sufficiency of perimeter lighting • Presence of obstructions, waste containers/material, combustibles, other risk factors • Evidence of vandalism, malicious damage, or other criminal activity • Maintenance schedules Number of security clearances undertaken Number of training courses and drills conducted

**Appendix II: Examples of Performance
Measures Used by Selected Organizations
outside of the Federal Government**

Security threats and general risks discussed at management forum and disseminated to all levels of agency staff

Security spending per square foot

Source: GAO.

Note: GAO analysis of data from state, local, and foreign government agencies and private-sector organizations.

Appendix III: Comments from the Department of Homeland Security

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



**Homeland
Security**

May 15, 2006

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

Dear Mr. Goldstein:

Re: Draft Report GAO-06-612, Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts (GAO Job Code 543129)

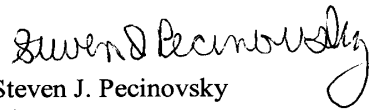
The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the Government Accountability Office's draft report. The report notes many of the challenges associated with developing and using meaningful performance measures. We concur with the overall findings and recommendations contained therein, and share your concern that without improved or additional means of measuring performance, it is difficult to assess the effectiveness and efficiency of efforts to protect Federal facilities.

DHS is implementing the requirements of Homeland Security Presidential Directive-7, *Critical Infrastructure Identification, Prioritization, and Protection*. As an essential part of that initiative, the Government Facilities Sector (GFS) is establishing performance measure guidance for federal, state, and local governments so they can better assess the effectiveness of their facility protection programs. The GFS is under the lead of the Federal Protective Service located within Immigration and Customs Enforcement. The Interagency Security Committee (ISC) is currently partnering with the GFS on that effort with respect to federal facilities, and will use it as the baseline for developing the recommended performance measurement guidance. We believe this is the most appropriate course of action to leverage limited resources and ensure consistency and timely completion of both tasks.

The ISC will include this task in its Action Plan for Fiscal Years 2007 and 2008, and will ensure that the performance measurement guidance reflects input from all ISC members and is distributed to all federal agencies. Progress, however, will be largely dependent on the availability of sufficient resources.

Technical comments will be sent under separate cover.

Sincerely,



Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Appendix IV: Comments from the Department of the Interior

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



United States Department of the Interior

OFFICE OF THE ASSISTANT SECRETARY
POLICY, MANAGEMENT AND BUDGET
Washington, DC 20240



MAY 15 2006

Mr. Mark L. Goldstein
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street, NW
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 *HOMELAND SECURITY, Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies Facility Protection Efforts (GAO-06-612)*, May 2006. In general, we agree with the findings, except as discussed in the enclosure, and we agree with the recommendations in the report.

The enclosure provides specific comments from the Department's Office of Law Enforcement and Security and the Office of Planning and Performance Management. We hope our comments will assist you in preparing the final report.

Sincerely,

R. Thomas Weimer
Assistant Secretary

Enclosure

**U.S. General Accountability Office Draft Report
Homeland Security: Guidance and Standards Are Needed for Measuring the
Effectiveness of Agencies Facility Protection Efforts
(GAO-06-612)**

Specific Comments:

Office of Law Enforcement and Security

(1) Pages 27-30

This section of the document refers to the Bureau of Land Management (BLM) conducting vulnerability assessments. This information regarding the BLM is incorrect and all reference to BLM should be removed from this section of the document. BLM has not been conducting the types of vulnerability assessments discussed in the report, and does not have a specialized physical security assessment methodology.

(2) Page 30

"However, the OLES officials told us that they do not have formal performance measures and targets for reducing the risk ratings." In April 2006, OLES developed and submitted for inclusion in the Departmental Strategic Plan performance measures related to the reduction in the percent of physical security vulnerabilities identified at departmental facilities.

General Comments:

Office of Planning and Performance Management

The report is unclear as to the value of a common set of government-wide facility protection performance measures and for whom this additional information would be directed. The report seems to express concern that there is not a single set of government-wide facility protection performance measures. A more critical need should be determining if each agency has effectively assessed and corrected its own facility vulnerabilities. Such an agency-by-agency assessment more effectively considers the different levels of criticality and protection needs of each facility in terms of its mission and individual condition, than could be covered by a cross-agency facility protection performance measure.

References to BLM have
been deleted.

See p. 34.

See comment 1.

See comment 2.

It is also not clear as to who is meant to be the recipient and benefactor of such a cross-agency assessment of facility protection performance. It is confusing in the report if GAO's concern is that there is not adequate information within agencies to make effective decisions about protecting their own facilities or if the results of this cross-agency assessment on facility protection is meant for public documents that would be related to implementation of the Government Performance and Results Act or the Program Assessment Rating Tool for publication on the OMB ExpectMore.Gov website. If the report is promoting a more public viewing of facility protection performance, it should also discuss any guidelines for ensuring that such information provides adequate accountability without revealing weaknesses or vulnerabilities that could be exploited. The GAO report needs to be clearer as for whom this information is targeted, guidelines for how such information could be made available and yet protected, and the value for expending the resources to collect this cross-agency information vs conducting a more direct internal agency-by-agency assessment of facility vulnerability and correction.

The following are GAO's comments on Interior's letter dated May 15, 2006.

GAO Comments

1. Interior suggested that an agency-by-agency assessment of each federal agency's facility vulnerabilities would be more effective than a cross-agency facility protection performance measure. We agree that identifying vulnerabilities and monitoring efforts to address those vulnerabilities is a useful part of an agency's comprehensive facility protection program. For example, the Department of Veterans Affairs conducts vulnerability assessments, and one Australian government agency we interviewed monitors the effect of different security investments on its facilities' risk ratings (which typically involve threat and vulnerability factors). However, we believe it is also important for decision makers to have comparable information about the relative security performance of facilities within an agency, rather than just in one bureau or service, as well as across the federal government. Such information could help reduce the risk of spending more money for less effective physical security or investing in the wrong areas.
2. Interior expressed concern that a more public viewing of agency facility protection performance could reveal weaknesses or vulnerabilities that could be exploited. We agree that this could be a concern, but choose to leave the development of guidelines for using and protecting such information to the Interagency Security Committee and its member agencies.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Mark Goldstein (202) 512-2834 or goldsteinm@gao.gov

Staff Acknowledgments

Other key contributors to this report were Roshni Davé, Tamera Dorland, Brandon Haller, Anne Izod, Jessica Lucas-Judy, Susan Michal-Smith, David Sausville, Scott Tessier, Candice Wright, and Dorothy Yee

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

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548