United States Government Accountability Office

GAO

Report to the Ranking Member, Committee on Homeland Security, House of Representatives

January 2013

FACILITY SECURITY

Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies

GAO-13-222

January 2013

FACILITY SECURITY

Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-222, a report to the Ranking Member, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

GAO has designated federal real property management as a high-risk area due, in part, to the continued challenge of facility protection. Executive branch agencies are responsible for protecting about 370,000 non-military buildings and structures; the Federal Protective Service (FPS) protects over 9,000 of these. ISC—an interagency organization led by the Department of Homeland Security (DHS)—issues physical security standards for agencies' use in designing and updating physical security programs. GAO was asked to review physical security programs at executive branch agencies with facilities that FPS does not protect. This report examines (1) the sources that inform agencies' physical security programs and (2) the management practices agencies use to oversee physical security and allocate resources. GAO reviewed and analyzed survey responses from 32 agencies. GAO also interviewed officials and reviewed documents from 5 of these agencies, which were selected as case studies for more in-depth analysis. The survey and results can be found at GAO-13-223SP.

What GAO Recommends

DHS should direct ISC to conduct outreach to executive branch agencies to clarify how its standards are to be used, and develop and disseminate guidance on management practices for resource allocation as a supplement to ISC's existing physical security standards. DHS concurred with these recommendations.

View GAO-13-222. To view the e-supplement online, click on GAO-13-223SP. For more information, contact Mark Goldstein at (202) 512-2834 or GoldsteinM@gao.gov.

What GAO Found

Agencies draw upon a variety of information sources in developing and updating their physical security programs. The most widely used source, according to survey responses from 32 agencies, is the institutional knowledge or subject matter expertise in physical security that agencies' security staff have developed through their professional experience. The second most used source are standards issued by the Interagency Security Committee (ISC). The standards, which are developed based on leading security practices across the government, set forth a decision-making process to help ensure that agencies have effective physical security programs in place. However, according to survey responses, the extent of agencies' use of ISC standards varied—with some agencies using them in a limited way. Agency officials from the case-study agencies said that certain conditions at their agencies—such as the types of facilities in the agencies' portfolios and their existing physical security requirements—contribute to limited use of the standards. ISC officials said that the standards are designed to be used by all agencies regardless of the types of facilities or their existing security programs; the standards can be customized to the needs of individual facilities and do not require the use of specific countermeasures. ISC has an opportunity to clarify how the standards are intended to be used when it trains agencies on them; during quarterly meetings with member agencies, where ISC can share best practices on the use of the standards; or when ISC engages in other outreach on the standards. Clarifying how agencies can use the standards may result in their greater use. Greater use of the standards may maximize the effectiveness and efficiency of agencies' physical security programs.

Agencies use a range of management practices to oversee physical security activities. For example, 22 surveyed agencies reported that they have a manager at the agency-wide level responsible for monitoring and overseeing physical security at individual facilities. In addition, 22 surveyed agencies reported that they have some documented performance measures for physical security. Such performance measures can help agencies evaluate the effectiveness of their physical security programs and identify changes needed to better meet program objectives. Agencies' use of management practices such as having a physical security manager responsible for allocating resources and using performance measures to justify investment decisions could also contribute to more efficient allocation of physical security resources across an agency's portfolio of facilities. However, some agencies make limited use of such practices to allocate resources. For example, only 13 reported that they have a manager for allocating resources based on risk assessments. In contrast, a majority of agencies reported having managers for other aspects of physical security, including those related to oversight. Greater use of management practices for allocating resources is particularly relevant given that the surveyed agencies identified allocating resources as the greatest challenge. As the government's central forum for exchanging information and disseminating guidance on physical security, ISC is well positioned to develop and disseminate guidance about management practices that can help agencies allocate resources across a portfolio of facilities. However, ISC's key physical security standards do not currently address management practices for allocating resources across an agency's entire portfolio of facilities.

Contents

Abbreviations

CCTV	closed-circuit television
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
FCC	Federal Communications Commission
FPS	Federal Protective Service
FRPP	Federal Real Property Profile
GSA	General Services Administration
Interior	Department of the Interior
ISC	Interagency Security Committee
OPM	U.S. Office of Personnel Management
USPS	U.S. Postal Service
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 24, 2013

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Dear Mr. Thompson:

Protecting federal facilities continues to be a challenge for agencies and is among the major reasons GAO designated federal real property management as a high-risk area.[1] In fiscal year 2010, federal executive branch agencies were responsible for protecting about 370,000 non-military buildings and structures.[2] Over 9,000 of these buildings and structures are protected by the Federal Protective Service (FPS). The remainder of the buildings and structures are protected by some three dozen other federal executive branch agencies.

The federal government's approach to physical security is largely decentralized, with individual agencies generally having the discretion to establish physical security programs that govern how they will protect their people, property, structures, and facilities. Agencies tailor these programs to their missions, the types of facilities they occupy, and other circumstances such as the level of public access needed and whether the facilities house classified or nuclear materials. The Interagency Security Committee (ISC)—an interagency organization led by the Department of Homeland Security (DHS)—is a central forum for standards and guidance

[1]GAO, *High Risk Series: An Update*, GAO-11-278 (Washington D.C.: February 2011). An update to GAO's *High Risk Series* will be forthcoming in February 2013.

[2]Federal Real Property Council, *FY2010 Federal Real Property Report*. The FY2010 report was the most recent report available during our review. The Federal Real Property Council's report provides summary-level information on government-wide real property data, as submitted by federal agencies to the Federal Real Property Profile (FRPP). The FRPP is a centralized real property database maintained by GSA that contains data on the federal government's real property inventory. The data that we provide on the number of buildings and structures exclude military assets. GAO has conducted previous work on the reliability of FRPP data, and has found problems with FRPP data collection practices. See GAO, *Federal Real Property: National Strategy and Better Data Needed to Improve Management of Excess and Underutilized Property*, GAO-12-645 (Washington D.C.: June 20, 2012). However, we found the FRPP data to be reliable for the purposes of providing a broad overview of the makeup of the government's federal real property portfolio.

that is available for agencies to consult when designing and updating their physical security programs. ISC is comprised of 51 federal agencies and departments, 21 of which are categorized as primary members that vote to approve the standards, and 30 of which are associate members that do not vote. ISC's purpose is to enhance the quality and effectiveness of security and the protection of buildings and facilities in the United States occupied by federal employees for nonmilitary activities. This report and Executive Order 12977,[3] which established the ISC, refer to buildings and facilities in the United States occupied by federal employees for nonmilitary activities as "federal facilities." ISC's purpose is also to provide a permanent body to address continuing government-wide security for these federal facilities.

GAO has completed a large body of work on FPS's protection of over 9,000 facilities.[4] However, given that many executive branch agencies are also responsible for the physical security of federal facilities, you asked us to examine the physical security programs at these agencies. The objectives of our review were to examine the (1) sources that inform how federal agencies conduct their physical security programs and (2) management practices that agencies use to oversee physical security activities and allocate physical security resources.

Our review focused on executive branch agencies that have non-military facilities in the United States and its territories that are not protected by FPS. To address our objectives, we conducted a web-based survey of 36 cabinet level and independent agencies; we received responses from all 36 agencies, which are listed in appendix II. Four agencies reported that all of their facilities were protected by FPS, and we therefore did not include them in our review. The remaining 32 agencies are included in our review, and in this report we identify these agencies as the agencies we surveyed. Of these 32 agencies, 16 are primary ISC members, 9 are

[3]60 Fed. Reg. 54411 (Oct. 24, 1995).

[4]Recent GAO reports on FPS include: GAO, *Federal Protective Service: Actions Needed to Assess Risk and Better Manage Contract Guards at Federal Facilities*, GAO-12-739 (Washington D.C.: Aug. 10, 2012); GAO, *Federal Protective Service: Better Data on Facility Jurisdictions Needed to Enhance Collaboration with State and Local Law Enforcement*, GAO-12-434 (Washington D.C.: Mar. 27, 2012); and GAO, *Federal Protective Service: Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS's Risk Assessment and Management Program*, GAO-11-705R (Washington D.C.: July 15, 2011).

associate ISC members, and 7 are not members of ISC. This report presents survey results in aggregate and does not discuss individual agency responses in a way that would identify them. Summary results for each survey question, except those requiring narrative responses, are available in a supplement to this report, GAO-13-223SP. We also conducted interviews with and reviewed documentation from officials at five case-study agencies for more in-depth analysis: the Department of Energy (DOE), the U.S. Postal Service (USPS), the Department of Veterans Affairs (VA), the Federal Communications Commission (FCC), and the U.S. Office of Personnel Management (OPM). We selected these agencies because they vary in the level of public access allowed at their facilities and the amount of building square footage they have. To obtain further information, we conducted site visits at DOE, VA, and USPS facilities in New Jersey, West Virginia, and Illinois, where we interviewed officials in charge of physical security at the facility and obtained documentation for review. We selected these locations and facilities to achieve diversity in geographic area, urban and rural environments, and facility risk levels. This report discusses the results of these case studies and site visits on an individual agency basis, in which case the agency referred to is identified by name, as well as in the aggregate. Since the five case-study agencies and the facilities we visited were selected as part of a non-probability sample, the findings from our case studies and facility visits cannot be generalized to all federal agencies. We also interviewed officials and reviewed physical security standards from the ISC and ASIS International, an organization for security professionals,[5] and reviewed GAO reports on facility protection and effective program management. See appendix I for more details on our scope and methodology.

We conducted this performance audit from November 2011 to January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[5]Founded in 1955 as the American Society for Industrial Security (ASIS), the organization officially changed its name in 2002 to ASIS International. ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests.

Background

The federal government's vast real property portfolio is used for all aspects of operations and includes buildings such as warehouses, office space, dormitories, and hospitals. Agencies' physical security programs address how agencies approach aspects of physical security for these buildings, such as conducting risk assessments to identify threats and vulnerabilities, determining which countermeasures to implement, and coordinating security efforts within the agency and with other agencies. We have previously reported that because of the considerable differences in types of federal facilities and the variety of risks associated with each of them, there is no single, ideal approach to physical security.[6] For example, in some instances, an agency's component offices—which are subordinate entities such as bureaus, administrations, or other operating divisions—have their own physical security programs for the facilities they use. In other instances, an agency's regions or districts play a role in physical security.

ISC was created by Executive Order 12977 in 1995, after the bombing of the Alfred P. Murrah federal building in Oklahoma City, to address physical security across federal facilities occupied by federal employees for nonmilitary activities.[7] ISC's mandate is to enhance the quality and effectiveness of security in and protection of federal facilities. To accomplish this, Executive Order 12977 directs the ISC to, among other things, develop and evaluate security standards for federal facilities, develop a strategy for ensuring compliance with such standards, and oversee the implementation of appropriate security measures in federal facilities. Executive Order 12977 also directs each executive agency and department to cooperate and comply with ISC policies and recommendations issued pursuant to the order.[8] The order, as amended,

[6]GAO, *Building Security: Security Responsibilities for Federally Owned and Leased Facilities*, GAO-03-08 (Washington, D.C.: Oct. 31, 2002).

[7]Initially, ISC was chaired by GSA. The Homeland Security Act of 2002 created DHS, and, in 2003, Executive Order 13286 amended Executive Order 12977 to transfer ISC from GSA to DHS. 68 Fed. Reg. 10619 (March 5, 2003).

[8]According to the executive order, executive agencies and departments are exempt from complying with ISC policies and recommendations if the Director of Central Intelligence determines that compliance would jeopardize intelligence sources and methods. In addition, individual agencies may have their own specific statutory authorities governing physical security requirements that may exempt them from complying with ISC policies and recommendations.

gives the Secretary of Homeland Security the responsibility to monitor federal agency compliance with ISC policies and recommendations.

Prior to the creation of ISC, there was no federal body responsible for developing government-wide physical security standards. Consequently, ISC became the government's central forum for exchanging information and disseminating standards and guidance on physical security at federal facilities. ISC's standards are intended to help agencies integrate security into the operations, planning, design, and construction of federal facilities and are intended to be customized to address facility-specific conditions. ISC has developed the following security standards and guidance, among others:[9, 10]

- *Physical Security Criteria for Federal Facilities* establishes a process for determining the baseline set of physical security measures to be applied at a federal facility and provides a framework for the customization of security measures to address unique risks at a facility.

- *Design-Basis Threat* establishes a profile of the type, composition, and capabilities of adversaries. It is designed to correlate with the countermeasures contained in the *Physical Security Criteria for Federal Facilities*.

- *Facility Security Level Determinations* defines the criteria and process to be used in determining the facility security level of a federal facility, a categorization that then serves as the basis for implementing ISC standards.[11]

- *Use of Physical Security Performance Measures* directs all federal agencies to assess and document the effectiveness of their physical security programs through performance measurement and testing.

[9]For a complete listing of ISC standards and guidance, see www.dhs.gov/interagency-security-committee-standards-and-best-practices. Accessed January 22, 2013.

[10]ISC officials said that they are in the process of consolidating and streamlining several of their physical security standards into a single document, which they believe will help facilitate agencies' use of the standards.

[11]*Physical Security Criteria for Federal Facilities, Design-Basis Threat*, *and Facility Security Level Determinations* have a status of For Official Use Only and are therefore not publicly available.

This standard provides guidance on how to establish and implement a comprehensive measurement and testing program.[12]

- *Security Specialist Competencies* provides the range of core competencies federal security specialists should possess to perform their basic duties and responsibilities.[13]

ISC's 51 member agencies meet quarterly to promote information sharing on physical security. Members serve on working groups and subcommittees to develop and update physical security standards and guidance, including those listed above. ISC also engages with industry and other government stakeholders to advance best practices and provides training on its standards to federal facility security professionals and other stakeholders. Leadership for the ISC is provided by DHS's Assistant Secretary for Infrastructure Protection, who is the chair of the ISC; an Executive Director; and eight standing subcommittees that identify long- and short-term priorities and oversee strategic initiatives.

Agencies' Physical Security Programs Are Largely Informed by Institutional Knowledge and ISC Standards

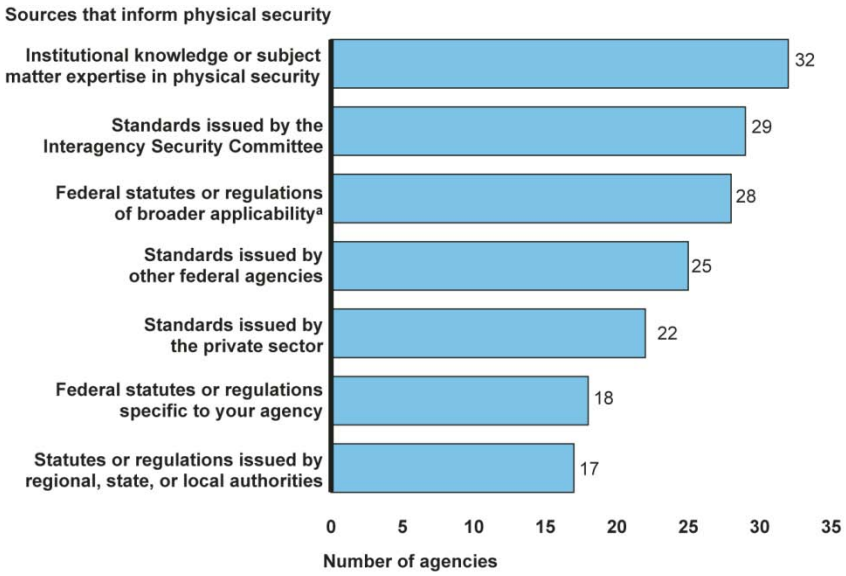
Agencies draw upon a variety of information sources in developing and continually refining aspects of their physical security programs, such as how and when to conduct risk assessments, what skills security staff should have, and how to determine which countermeasures to implement at their facilities. Sources can include an agency's institutional knowledge or subject matter expertise in physical security, federal statutes and regulations, physical security standards issued by ISC, and state or local regulations, among others, as shown in figure 1. Characteristics such as agencies' missions and the type, use, and location of their facilities can affect which of these sources agencies use. For example, a facility may adhere to local building codes that affect aspects of physical security such as perimeter fencing, or a facility that is used to house radioactive waste may be subject to federal requirements on the storage of nuclear materials. Institutional knowledge in physical security and ISC's physical security standards were the two sources that our survey results and case-

[12]Department of Homeland Security, Interagency Security Committee, *Use of Physical Security Performance Measures* (Washington, D.C.: 2009).

[13]Department of Homeland Security, Interagency Security Committee, *Security Specialist Competencies, An Interagency Security Committee Guideline*. 1st edition (2012).

study interviews showed to be the most influential in guiding agencies' physical security programs.[14]

Figure 1: Agencies Reported That the Following Sources Inform Their Physical Security Programs



Source: GAO survey of federal agencies.

Note: Thirty-two agencies responded to the survey question on whether they used any of the sources in the figure above to inform their physical security programs.

[a]Federal statutes or regulations of broader applicability are those that apply to multiple agencies rather than being specific to one agency.

[14]As shown in figure 1, agencies we surveyed cited federal statutes and regulations of broader applicability to be the third most influential source for guiding agencies' physical security programs. However, when we surveyed agencies about whether they use this source to inform the specific aspects of physical security as shown in figure 2, a fewer number of agencies we surveyed cited that they used this source as compared to institutional knowledge and ISC standards. Consequently, this objective focuses on agencies' use of the two most used sources—institutional knowledge and ISC standards—and not on the use of federal statutes and regulations. Assessing agencies' compliance with federal statutes and regulations was outside the scope of our work. Survey results on use of federal statutes and regulations and other sources can be found in GAO-13-223SP.

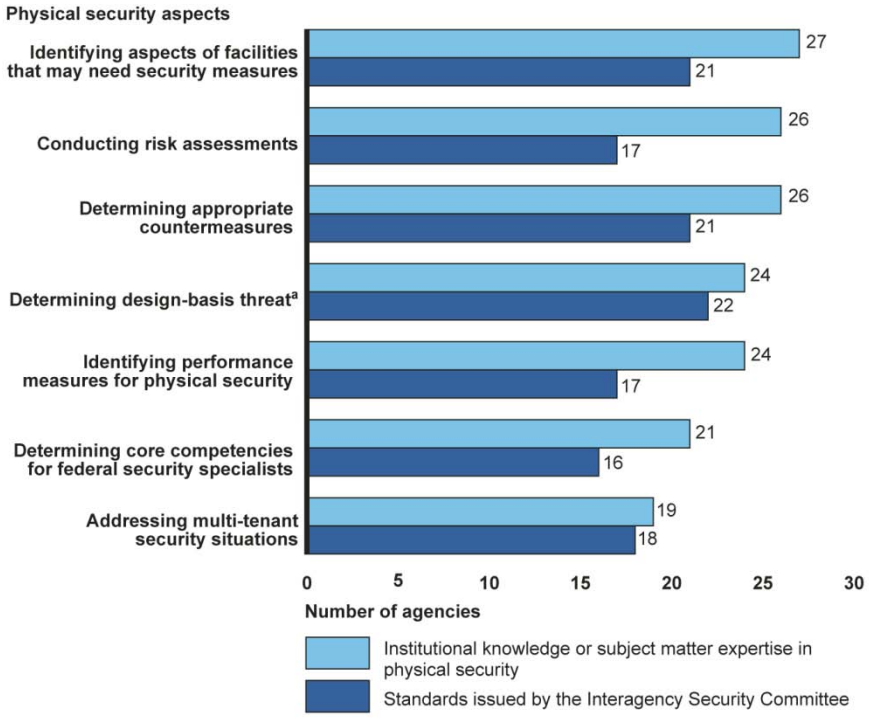
Institutional Knowledge, Subject Matter Expertise in Physical Security, and Prior Security Experience Inform Agencies' Physical Security Programs

All 32 of the agencies we surveyed reported that institutional knowledge or subject matter expertise informs their physical security programs. This was the most widely used source cited in our survey, as shown in figure 1. For example, officials from three of the agencies we surveyed said that the knowledge, experience, and expertise that their security specialists have in physical security—which they consider institutional knowledge—is reflected in their physical security programs and policies. One of these officials said his agency contracts with a security company that has extensive knowledge and experience in providing security and law enforcement to high profile institutions across the federal government, and that this knowledge is used in managing the agency's security program. Another agency official said that the knowledge gained from employees' previous education, training, or work experiences, or historical knowledge of the agency has assisted in the development of several security policies and procedures within the agency.

Agencies also rely heavily on institutional knowledge or subject matter expertise to inform specific aspects of their security programs, more so than any other source we asked about in our survey. As shown in figure 2, 26 agencies reported that institutional knowledge informs how they conduct risk assessments and determine appropriate countermeasures. For example, officials from two of our case-study agencies—DOE and USPS—said that they use institutional knowledge to inform how they conduct these activities. DOE headquarters officials told us that when developing and updating agency-wide physical security policies, which address topics such as risk assessments, they obtain input from DOE staff in their component offices,[15] who have knowledge of the particular needs and constraints of their facilities based on their experience implementing security programs. In addition, USPS officials said that their security staff's knowledge of the agency's long-standing security program and their professional education in physical security helps them make decisions about security measures needed at their facilities, such as on the location of perimeter fencing and the appropriate brightness for security lights.

[15]Component offices are subordinate entities within an agency, such as bureaus, administrations, and other operating divisions within an agency. At DOE, component offices include the Office of Science and the Office of Fossil Energy.

Figure 2: Agencies Reported That the Following Physical Security Aspects Are Largely Informed by Institutional Knowledge or Subject Matter Expertise and Standards Issued by the ISC



Source: GAO survey of federal agencies.

Note: Thirty agencies responded to the survey question on how institutional knowledge informed key aspects of physical security. Two of the agencies reported in a separate survey question that they use institutional knowledge, in general, to inform their physical security programs but did not answer the survey question on individual aspects of security. Twenty-nine agencies responded to the survey question on how ISC standards informed key aspects of physical security.

[a]Design-basis threat is an approach that helps agencies establish the type, composition, and capabilities of adversaries across a range of their facilities.

Most Agencies Use ISC Standards, but Only Some Rely Extensively on Them

Twenty-nine of 32 agencies surveyed reported that ISC standards inform their physical security programs, making it the second most-used source behind institutional knowledge, as shown in figure 1. Officials we interviewed from our case-study agencies said that they use ISC standards as one of many sources that inform what they include in their physical security programs. ISC has developed a number of government-wide physical security standards that address topics intended to help guide agencies' physical security programs, including determining a facility's risk level and identifying threats posed by potential adversaries, among other things. Agencies' use of ISC standards can help ensure that

physical security programs are effective government-wide. The standards are developed based on the collective knowledge and physical security expertise of ISC member agencies and, therefore, reflect leading practices in physical security. Every ISC member agency that we surveyed, as well as four agencies that are not ISC members, reported that they use ISC standards at least to some degree. The three agencies we surveyed that reported that they do not use ISC standards at all are not ISC members.[16] According to our survey, ISC standards are most often used for conducting design-basis threat analysis of agency facilities, identifying aspects of facilities that need security measures, and determining appropriate countermeasures, as shown in figure 2.

Although the majority of agencies we surveyed use ISC standards, the extent of their reliance varies—with some agencies using the standards extensively to inform their physical security programs and some using them in a more limited way. For example, 11 agencies reported that all of the physical security aspects shown in figure 2 are largely informed by ISC standards, whereas six agencies reported that none of these aspects are largely informed by ISC standards.[17] Instead, these six agencies generally reported that these aspects are somewhat, minimally, or not informed by ISC standards. Among the six agencies that said none of these aspects are largely informed by ISC standards, three are primary ISC members, two are associate members, and one is not an ISC member.

We found that agencies' reasons for making limited use of ISC standards reflect a lack of understanding by some agencies regarding how the standards are intended to be used. For example, officials from the case-study agencies that we interviewed said that certain conditions at their agencies contribute to their limited use of the standards. Specifically, these agencies cited the suitability of the ISC standards to the agencies' facilities and their own physical security requirements as contributing to their limited use of the standards.

[16]These three agencies are small real-property-holding agencies in terms of the number of buildings and structures and total building square footage.

[17]The remaining 12 agencies reported that the ISC standards largely inform at least one but not all physical security aspects.

- *Suitability of standards*. Officials we interviewed at our case-study agencies told us that they are selective in their use of ISC standards because the standards are not suitable for the types of facilities in their portfolio. For example, USPS officials said that, consistent with ISC standards, they establish a baseline level of protection at their facilities that address facility-specific functions and threats, but they do not follow some practices included in the ISC standards—particularly those related to access control—because the practices are not suitable for the high degree of public access needed at post offices. Likewise, VA officials told us that they do not use ISC standards for all of their facilities because some practices included in the standards do not cover security topics that are specific to their facilities, such as hospitals and health clinics.[18] In response to these comments, ISC officials told us that ISC's standards are designed to be suitable for all facilities and to accommodate a broad range of security needs, conditions, and types of facilities. For example, *ISC's Physical Security Criteria for Federal Facilities*—one of ISC's key standards—establishes a decision-making process to help agencies consistently determine the baseline level of protection needed for each facility. The *Criteria* provide agencies the flexibility to build upon or customize the baseline level of protection to address facility-specific conditions. According to the *Criteria*, consistency in the process used to determine a baseline level of protection for each facility is important because it helps ensure that the risks that all facilities face—regardless of the type facility—are mitigated to an acceptable level. Furthermore, according to ISC officials, the *Criteria* do not prescribe specific countermeasures and, as a result, can be used by all agencies regardless of the type of facilities in their portfolio.

- *Use of other physical security standards*. Officials we interviewed at our case-study agencies also told us that they do not make greater use of ISC standards because they have their own standards for physical security. For example, officials at DOE told us that the Atomic Energy Act was the foundation for their security program long before the ISC was created and ISC standards developed. Additionally, DOE officials told us that the act and DOE's security policy derived from it establishes physical security requirements for their facilities with

[18]VA officials told us that one exception is for Veterans Benefits Administration facilities that are under the custody and control of GSA. For these facilities, the officials said that they use ISC standards.

classified or nuclear material and that these requirements are usually more stringent than ISC requirements. Similarly, VA officials told us that they have developed their own physical security standards that are specific to the needs of their hospital and clinic facilities, and that these standards go above and beyond ISC standards. ISC officials told us that, because ISC standards are intended to ensure a minimum or baseline level of protection, it is appropriate for agencies to have their own requirements and standards that exceed those of ISC. According to ISC officials, an agency should apply the decision-making process established by the ISC standards to determine if their facilities' physical security requirements meet the baseline, and then add additional requirements based on their agency's needs.

As previously discussed, ISC was established to enhance the quality and effectiveness of security in and protection of non-military, federal facilities. Although most agencies we surveyed use ISC standards to some degree, some agencies' use of the standards is limited because they believe that the ISC standards are not suitable for their circumstances. Clarifying how agencies can use the standards regardless of the types of facilities in their portfolio and in concert with their existing physical security programs may result in the greater use of the standards. Use of ISC standards may be beneficial because they provide agencies with tools and approaches for consistently and cost-effectively establishing a baseline level of protection at all facilities commensurate with identified risks at those facilities. By using the standards to determine the level of protection needed to address the unique risks faced at each facility, agencies may be able to avoid expending resources on countermeasures that are not needed.

ISC currently does not formally monitor agencies' compliance with ISC standards. ISC officials said that with only five full time employees and a budget that is not a dedicated line item within DHS's budget, it lacks the staff and resources to conduct monitoring. Currently, in place of a formal monitoring program, ISC officials hold quarterly meetings and participate in ISC working groups along with their member agencies. ISC officials said that the information sharing that occurs through these channels helps them achieve a basic understanding of whether and how member agencies use the standards. This approach, however, does not provide a thorough or systematic assessment of ISC member agencies' use of the standards, and provides no information on non-member agencies' physical security practices. Further, because ISC conducts limited outreach to non-member agencies, property-holding agencies that are not ISC members may not be fully aware of the benefits that the use of the

ISC standards might have for them. ISC stated in its 2012 to 2017 action plan that it plans to establish protocols and processes for monitoring and testing compliance with its standards by fiscal year 2014.[19] According to ISC's executive director, monitoring agencies' compliance with the standards could include agency self-assessments or ISC officials' assessing agencies' compliance. Monitoring and testing as well as other methods of measuring the performance of the standards can help gauge the adequacy of facility protection, improve security, and ensure accountability for achieving the goals of the standards.[20]

In commenting on a draft of this report, DOE and USPS stated that they use ISC standards as a baseline for at least some of their facilities. DOE officials said that ISC standards must be considered the baseline for security for facilities that do not have classified or nuclear material but have federal personnel. USPS officials said that ISC's *Criteria* standard provides flexibility to customize baseline levels of protection to address facility-specific conditions and that it is within this framework that USPS employs appropriate countermeasures at its facilities when it is not able to adopt ISC's recommended standards. As discussed, ISC is planning to monitor and test agencies' compliance with ISC standards. This monitoring and testing will help shed more light on whether these and other agencies' approaches align with ISC's standards.[21]

[19]Department of Homeland Security, *Interagency Security Committee Action Plan 2012-2017*.

[20]Our previous reports on key practices and performance measurement for facility protection discuss elements that contribute to effective measures of performance. See GAO-05-49 and GAO, *Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts*, GAO-06-612 (Washington, D.C.: May 31, 2006).

[21]We did not assess whether agencies comply with ISC standards as this was outside the scope of this review.

Agencies Use a Range of Management Practices to Oversee Physical Security Activities, but Make Limited Use of These Practices to Help Allocate Resources

Agencies Use Several Management Practices to Oversee Physical Security and Ensure Program Effectiveness

Based on responses to our survey and our interviews with agency officials, we found that agencies use a range of management practices that can contribute to effective oversight of physical security programs, including:

- having a manager responsible for physical security,
- having agency-wide physical-security policies,
- using risk management[22] practices that compare physical security across facilities, and
- measuring the performance of physical security programs.[23]

We and others have reported that these practices can help agencies address risks, achieve effective results in their programs, determine program effectiveness, and identify whether changes are needed to better meet the program objectives.

Physical Security Manager

A physical security manager can be beneficial for an agency because the manager can establish a cohesive strategy for the agency to mitigate or reduce risk across the agency's facilities, coordinate and oversee

[22]Risk management generally involves identifying potential threats, assessing vulnerabilities, identifying the assets that are the most critical to protect in terms of mission and significance, and evaluating mitigation alternatives for their likely effect on risk and cost.

[23]The other practices we asked about in our survey include leveraging technology, strategic human capital management, and information sharing and coordination. Results on agencies' use of these practices can be found in GAO-13-223SP.

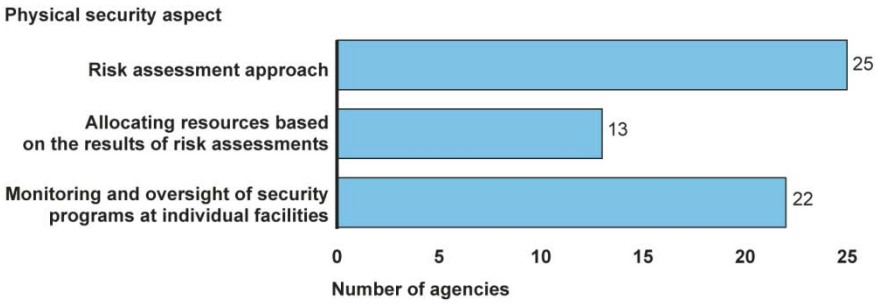
physical security efforts across departments, and minimize potential redundancies that could be occurring across departments if accountability for physical security is dispersed among several managers, according to guidance issued by ASIS International.[24]

Many of the agencies we surveyed reported that they have a manager at the agency-wide level responsible for their risk assessment approaches and monitoring and oversight (25 and 22 agencies, respectively), as shown in figure 3. However, we determined that physical security managers at our case-study agencies have varying levels of responsibility. For example, DOE's director of security has agency-wide responsibility and works with component offices throughout the agency to ensure that the component offices' security programs align with DOE policies, which helps achieve a consistent approach to security across the agency. Alternatively, FCC's chief security officer is responsible for physical security at only a select group of the 14 facilities held by FCC. Two of FCC's component offices are responsible for physical security at the remaining facilities. Each of these component offices approach physical security in a way that meets its particular needs. The FCC official we interviewed acknowledged, however, that if physical security were centrally managed—through a physical security manager with agency-wide responsibilities, for example—the agency could benefit from a consistent approach to physical security for facility types that are similar. Although it is important to tailor physical security to facilities so that the unique risks at those facilities are addressed, a consistent approach to certain aspects of physical security is beneficial because it helps ensure that all facilities are covered by a baseline level of physical security commensurate with identified risks at those facilities. For example, we previously reported that the Department of the Interior (Interior) established a central law enforcement and security office in 2002 that enabled it to develop a uniform risk assessment and ranking methodology to quantify risk, identify needed security enhancements, and measure risk-reduction benefits at some of its properties. In addition to fostering consistency, a central approach to physical security can also help coordinate physical security across component offices and provide a single point of contact for the agency for physical security. For example, Interior's central office responsible for security provided the agency with a

[24]ASIS International, *Chief Security Officer Guideline,* 2008 Edition (2008).

single point of contact that the Secretary and senior managers could depend upon for security information and advice.[25]

Figure 3: Agencies Reported That They Have a Manager at the Agency-Wide Level Responsible for the Following Aspects of Physical Security



Source: GAO survey of federal agencies.

Note: Thirty agencies provided responses to the survey question on whether they have a unified manager responsible for the physical security aspects in the figure above.

Agency-Wide Physical Security Policies

We have previously reported that agencies' physical security programs can benefit from documented agency-wide guidelines. According to GAO's *Standards for Internal Control in the Federal Government*,[26] policies and procedures that enforce management's directives at an agency-wide level are an important part of an agency's ability to achieve effective results in its programs, in physical security as well as other types of programs. Furthermore, according to the *Standards for Internal Control*, assessing compliance to policies and procedures can also assist agencies in monitoring and measuring the performance of programs, including physical security programs.

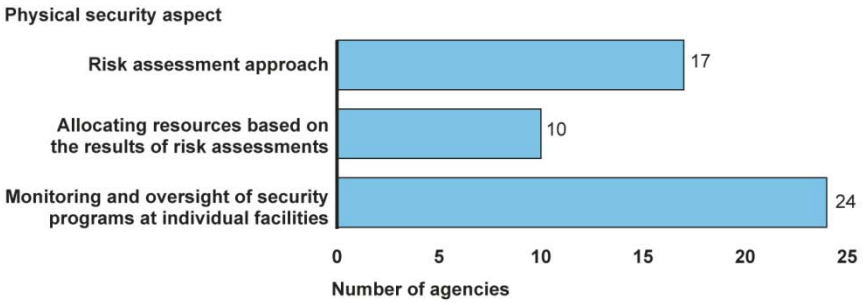
A majority of the agencies (24) we surveyed reported that they have documented agency-wide guidelines for monitoring and overseeing security programs at individual facilities, as shown in figure 4. Our more in-depth analysis of the case-study agencies found that they have documented agency-wide policies for a range of physical security activities. For example, DOE has documented policies for facility-level security plans, performance assurance, facility clearance activities, and

[25]GAO-09-983.

[26]GAO, *Internal Control: Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

other security-related activities that apply to individual facilities, and according to OPM officials their agency has a documented general security policy and access control policy. Having documented policies can help agencies ensure that their security programs achieve results. For example, USPS's security policy states that its security policies and adherence to these policies can help the agency ensure that the most appropriate level of security and protection available are provided to its facilities. DOE's security policy states that adherence to the policies can help prevent adverse impacts on the safety of DOE and contractor employees and the public.

Figure 4: Agencies Reported That They Have Documented Agency-Wide Guidelines for the Following Aspects of Physical Security



Source: GAO survey of federal agencies.

Note: Twenty-nine agencies provided responses to the survey question on whether they have documented agency-wide guidelines for the physical security aspects in the figure above.

Most agencies (26 of 32) we surveyed reported that offices at the agency-wide or component level, or both, monitor facilities' compliance with policies and procedures. In addition, six agencies reported that their region or district offices or facilities are responsible for performing this activity, rather than agency-wide or component offices. Agency-wide offices at our case-study agencies monitor facilities' compliance with agency-wide policies. For example, USPS staff working in field offices annually assess whether postal facilities are complying with agency-wide policies, and the headquarters security office reviews the results of the assessments. At DOE, component offices assess facilities' compliance with security policies and the agency-wide security office reviews high risk facilities to determine if DOE policies have been adequately implemented.

Risk Management

We have previously identified risk management as a key practice in facility protection.[27] A risk management approach that compares physical security across facilities can provide agencies assurance that the most critical risks at facilities across their agencies are being prioritized and mitigated, and that systemic risks are identified and addressed.

Agencies we surveyed reported that they conduct risk management practices—such as comparing risk assessments across facilities and monitoring the implementation of countermeasures across facilities—and that such practices are most often the responsibility of agency-wide offices, component level offices, or both. Specifically, of the 32 agencies we surveyed, 24 agencies reported that agency-wide or component offices, or both, had primary responsibility for comparing risk assessments across facilities and 26 agencies reported that either or both of these offices had primary responsibility for monitoring countermeasure implementation across facilities. A few agencies reported that regional or district offices or facilities had primary responsibility for these activities instead of agency-wide or component offices.[28] However, not all agencies we surveyed perform these activities: six agencies reported that they do not compare risk assessments across facilities, and two agencies reported that they do not monitor the implementation of countermeasures across facilities. Officials from OPM and DOE, two of our case-study agencies, said that they do not compare risk assessments across facilities. Specifically, OPM officials told us that they do not compare the results of the risk assessments across facilities because they have a small facility portfolio and have not seen the need to do such a comparison. Rather, the agency uses risk assessments to determine what countermeasures need to be implemented to address risks at individual facilities. Similarly, DOE officials told us that each of their component offices conducts risk assessments in different ways and that the Office of Health, Safety, and Security, which has agency-wide responsibility for physical security policy and oversight, does not compare

[27]GAO, *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).

[28]Two agencies reported that regional or district offices, or facilities were responsible for comparing risk assessments, and four agencies reported that these offices or facilities were responsible for monitoring countermeasure implementation.

risks across components or facilities.[29] In contrast, officials from another case-study agency, USPS, said that they do perform such comparisons. USPS officials who have agency-wide responsibilities for physical security said that they review the results of risk assessment performed across facilities to identify trends or anomalies that may indicate a systemic problem, and use this information to determine which countermeasures need to be implemented on a national basis. Monitoring the implementation of countermeasures across facilities can provide agencies with an agency-wide understanding of their vulnerabilities and whether identified risks have been mitigated.

Measuring Program Performance

Another key practice in facility protection we have identified is the use of performance measures.[30] In the area of physical security, performance measures could include the number of security incidents or the effectiveness of countermeasures, among other things. We have previously reported that benefits of performance measures for physical security include helping agencies reach their strategic objectives for physical security, evaluating the effectiveness of their physical security programs, and identifying changes needed to better meet the program's objectives.[31]

Twenty-two of 32 agencies we surveyed reported that at least some of their performance measures are documented in agency-wide or component-level planning, budget, or performance reports.[32] The remaining 10 agencies reported that they did not have or did not know if they have performance measures documented in such reports.[33] One of our case-study agencies, OPM, uses agency-wide performance

[29]In commenting on a draft of this report, DOE officials stated that while they do not compare risk assessments across their facilities, DOE does require, for high consequence facilities, formal risk acceptance by management officials based on the results of risk and vulnerability assessments.

[30]GAO-05-49.

[31]GAO-06-612. ISC has also emphasized the importance of performance measures for physical security. See Department of Homeland Security, Interagency Security Committee, *Use of Physical Security Performance Measures* (Washington, D.C.: 2009).

[32]Performance measures are often aligned with an agency's strategic plan, or can be included in an agency's performance reports.

[33]Four of these 10 agencies reported that the survey question on documented performance measures was not applicable to them.

measures to measure the performance of its security program. In contrast, officials from another case-study agency, DOE, said that such measures are difficult to implement at their agency. OPM, for example, has specific goals for its physical security program that are reflected in the evaluation used for its director of security. These performance goals, which are linked to the agency's strategic plan and operational goals, include measures such as completing a certain number of facility risk assessments, revising physical security policies, and fully implementing physical security technologies by specific dates. In contrast, DOE officials told us that although measuring performance on an agency-wide basis is a beneficial practice, they do not have agency-wide performance measures because each DOE facility varies, making it difficult to compare performance trends across facilities.

Agencies Make Limited Use of Management Practices for Allocating Resources

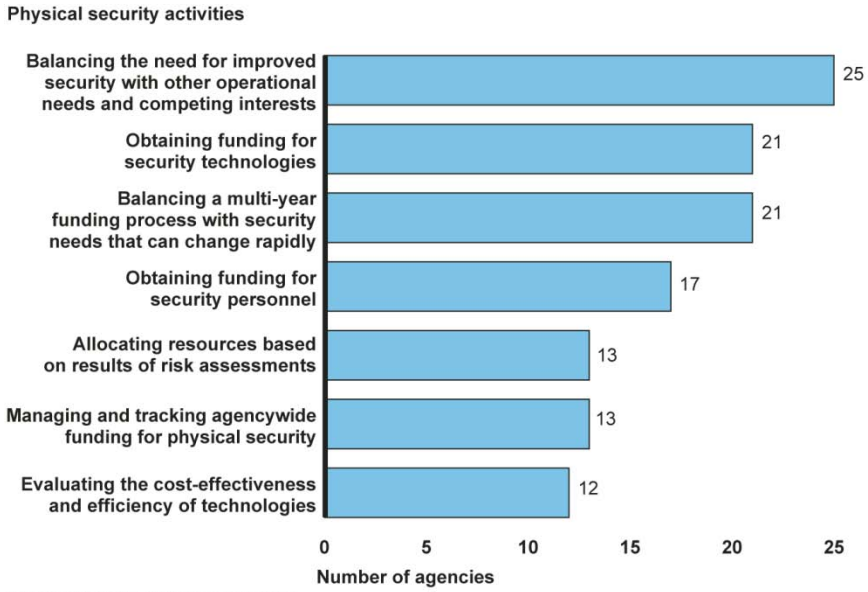
Among the physical security activities we asked about, agencies we surveyed identified allocating physical security resources across an agency's portfolio as the greatest challenge.[34] A majority of agencies (17 or more) we surveyed identified the following resource allocation activities as extremely or very challenging: balancing the need for improved security with other operational needs and competing interests, obtaining funding for security technologies and personnel, and balancing the funding process with changing security needs. Additional activities related to resource allocation were also among those that surveyed agencies found most challenging, as shown in figure 5. Surveyed agencies generally reported other aspects of physical security that we asked about to be less challenging than those related to resource allocation.

Officials we interviewed at various levels in our case-study agencies—including at agency-wide offices and facilities—also cited challenges related to the timeliness of funding decisions or prioritizing resource allocation decisions. For example, DOE officials in the agency-wide office responsible for physical security said that once they decide which countermeasures they need to implement to address threats or vulnerabilities, it takes time to obtain funding because the budget cycle spans multiple years. Similarly, officials at a USPS facility we visited said

[34]We surveyed agencies on whether they found 30 physical security activities to be extremely, very, moderately, somewhat or not challenging, or whether they had no opinion. See GAO-13-223SP for a list of the challenges and a summary of agencies' responses.

that USPS's funding process—which involves headquarters prioritizing security funds and reassessing the priorities during the year to take into consideration newly identified security deficiencies—makes it a challenge for the facility to obtain funding as quickly as it would like. A USPS headquarters official said that this might occur because there are other facilities that have higher priority security needs, and that facilities would be able to implement an interim solution while awaiting funding for a long-term solution. Officials must also prioritize funding for physical security along with other agency needs, as described by an official from a VA hospital we visited, who said that the medical center director has to balance funding for physical security needs, such as training for security personnel, with other hospital needs, such as medical equipment and overtime pay.

Figure 5: Agencies Reported the Following Resource Allocation Activities as Extremely or Very Challenging



Source: GAO survey of federal agencies.

Note: Thirty-two agencies responded to the survey questions on how challenging they found physical security activities. We asked agencies whether each physical security activity was extremely, very, moderately, somewhat, or not challenging, or whether they had no opinion.

Agency officials we interviewed at our case-study agencies said that the following circumstances contribute to the challenges they experience in allocating physical security resources:

- *Evolving threats*. DOE officials at the agency-wide level and a component office discussed the budgetary implications of the need to address constantly changing threats and increased risks, which results in the need for new or increased countermeasures at their facilities. For example, the agency-wide officials said that after the terrorist attacks of September 11, 2001, there was a large focus on security and that as a result, DOE incorporated many new countermeasures at its facilities. The officials stated that the threats have changed over time, and different countermeasures are required to address the new threats.

- *Limited familiarity with aspects of physical security*. A USPS headquarters official said that his agency recently took steps to help individuals who make funding decisions in physical security make more informed funding decisions. This official said that USPS improved the existing level of coordination between the individuals responsible for making funding decisions and those with expertise in physical security. According to USPS, this enabled the agency to more effectively prioritize and decide which physical security projects should get funded. Likewise, a police officer at a VA facility we visited described the challenge of identifying appropriate and cost-effective technologies to purchase because his training and expertise are in law enforcement, not in technological aspects of physical security.

- *Limited budgets available for physical security*. Agencies throughout the federal government have experienced or are experiencing budget constraints that have limited the funding available for their programs, including physical security programs. Agency officials we interviewed told us that they have limited funds to implement some physical security measures that address identified risks. A USPS official we interviewed said that while baseline physical security measures are in place at each USPS facility, financial constraints, caused by declining revenues at the agency, have affected the agency's ability to deploy security enhancements at its facilities. For instance, because of limited funding, implementing security enhancements, such as an upgraded closed-circuit television (CCTV) system, may be delayed at a facility until the needed funding becomes available. In addition, an official at FCC stated that funding was not available to implement several recommendations identified in its fiscal year 2012 physical security risk assessments. This official said that while there has not been an immediate impact of not funding these recommendations, the lack of funding results in continued risks not being addressed. However, in instances when a risk assessment identified an

immediate or imminent threat, this official said that funding was made available to mitigate or reduce the threat.

As discussed, agencies are already using management practices to support oversight of their physical security programs, but according to our survey, agencies make limited use of some of these management practices for the purposes of allocating resources. For example, as shown in figure 3, of the 30 agencies responding to the survey question on whether they have a manager responsible for physical security aspects we asked about, only 13 reported that they have a manager for allocating resources based on risk assessments.[35] In contrast, a majority of agencies reported having managers for other aspects of physical security, including those related to oversight. In addition, as discussed, 6 agencies do not compare risk assessments across facilities and 10 agencies do not have or do not know if they have documented agency- or component-wide performance measures. In addition to supporting oversight, we identified a number of examples of how agencies' use of management practices can contribute to more efficient allocation of physical security resources across an agency's portfolio of facilities. Below are examples of how management practices—such as having a physical security manager, comparing risk assessments across facilities, and using performance measures—can aid in more efficient resource allocation. The use of management practices for the purposes of resource allocation is particularly relevant given the challenges cited in this area.

- DOE's Office of Inspector General recently reported that the agency could realize efficiencies by consolidating security guard contracts from multiple offices throughout the agency to a single unified office. A physical security manager who is responsible for allocating resources across an agency or across components within an agency can help bring about greater efficiencies in procurement of equipment or personnel at the agency.

- We have previously reported that comparing physical security across facilities, such as comparing the results of risk assessments across facilities and monitoring the implementation of countermeasures across facilities, is another risk management practice that can help

[35]In commenting on a draft of this report, DOE officials stated that it would not be practical to have a single resource manager at their agency because physical security funds are allocated to various component offices as specific budget line items.

agency officials prioritize resource allocation decisions.[36] In this context, USPS headquarters officials said that they are in the process of improving their capability to compare the results of risk assessments across facilities. They plan to use these comparisons to help them prioritize which facilities in their portfolio have the greatest physical security needs and then direct funding to meet the priority needs.

- We have also previously reported that using physical security-related performance measures can help agencies justify investment decisions to maximize available resources.[37] Such performance measures have helped security officials in one government agency in Australia allocate resources more effectively across facilities. One performance measure this agency used allowed 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. Security officials then used the results to justify spending decisions and prioritize security investments.[38] Although this example is from an agency outside of the United States, the use of such performance measures could be a useful practice to more effectively allocate resources at agencies within the United States as well.

As the government's central forum for exchanging information and disseminating guidance on physical security at federal facilities, ISC is well positioned to develop and disseminate guidance on management practices that can help agencies make funding decisions across a portfolio of facilities. ISC's key physical security standards can help agencies make resource allocation decisions at individual facilities, but the standards do not currently address management practices for allocating resources across an agency's entire portfolio of facilities. ISC's key standards—*Facility Security Level Determinations, Physical Security Criteria*, and *Design-Basis Threat*—are intended to be used to determine the types of countermeasures needed at a given facility to provide a baseline level of protection. In this regard, the standards can help

[36]GAO-10-142.

[37]GAO-06-612.

[38]GAO-06-612.

agencies make spending decisions at individual facilities, but do not provide direction to guide funding decisions across a portfolio of facilities. ISC officials we interviewed said that compiling information on management practices that support the allocation of resources across a portfolio of facilities would be useful for agencies.

Conclusions

Agencies' physical security programs are mainly informed by their own institutional knowledge and subject matter expertise and, to a lesser degree, ISC standards. A few agencies rely extensively on ISC standards to inform key aspects of their security programs, but others use the standards in a more limited way. Agencies whose officials we interviewed and those we surveyed told us that they do not use ISC standards to a greater degree because the standards are not suitable to their facilities or because their agencies base their security programs on their own physical security standards that they believe obviate the need to use ISC standards. These reasons indicate some agencies lack an understanding of how the standards are intended to be used. As ISC officials stated, the standards are meant to accommodate almost any type of facility and are to be used in concert with other physical security requirements to which agencies may be subject. ISC has an opportunity to clarify to agencies how the standards are intended to be used when it disseminates new or updated standards, provides training to agencies on the standards, or engages in other outreach regarding the standards. Furthermore, ISC can use its quarterly meetings with its member agencies as a forum to share best practices on how the standards are to be used. Such outreach to clarify how the standards can be used may result in the greater use of the standards by ISC member agencies. Likewise, outreach by ISC to executive branch agencies that are not ISC members to clarify how the ISC standards are to be used may also lead to wider adoption of ISC standards. Potential benefits of more widespread use of ISC standards include helping to achieve the purpose of Executive Order 12977 to enhance the quality and effectiveness of security of federal facilities. Moreover, consistent use may help ensure that federal agencies are following a decision-making process that helps ensure that all facilities are covered by a cost-effective baseline level of protection commensurate with identified risks at those facilities. In addition to these benefits, clarifying to executive branch agencies how ISC standards are to be used will also help the agencies understand what the standards require, which is an important first step for ISC as it prepares to monitor and test agencies' compliance with its standards.

Government agencies are faced with increasing security requirements and limited budgets. Effective program management, including the use of management practices such as risk management strategies and a centralized management structure, can help make the most effective use of limited resources. While agencies are already using management practices to support oversight of their physical security programs, agencies make limited use of some of these management practices for the purposes of allocating resources. For example, most agencies do not have a central manager or agency-wide guidelines for allocating resources across facilities based on risk assessments, and some agencies do not compare risk assessments across facilities. Agencies also reported that the greatest challenge they face—among the physical security activities we asked about—is allocating physical security resources. ISC's key standards do not currently provide guidance on management practices that agencies can use to allocate resources across their entire portfolio of facilities. Agencies' use of management practices could help agencies make resource allocation decisions strategically for their entire portfolios of facilities and maximize effective resource allocation agency-wide. As the government's central forum for exchanging information and disseminating guidance on physical security at federal facilities, ISC is well positioned to develop and disseminate guidance that could increase agencies' use of these practices.

Recommendations

We recommend that the Secretary of Homeland Security direct ISC to take the following two actions:

- To help achieve the purpose of Executive Order 12977 to enhance the quality and effectiveness of security of federal facilities, conduct outreach to all executive branch agencies to clarify how the standards can be used in concert with agencies' existing physical security programs.

- To help agencies make the most effective use of resources available for physical security across their portfolios of facilities, develop and disseminate guidance on management practices for resource allocation as a supplement to ISC's existing physical security standards. This effort could include identifying practices most beneficial for physical security programs and determining the extent to which federal agencies currently use these practices.

Agency Comments

We provided a draft of this report and the e-supplement that provides summary results of our survey to DHS, DOE, VA, USPS, FCC, and OPM for comment.[39] In written comments, reproduced in appendix III, DHS concurred with the report's recommendations. DHS said that ISC would conduct outreach with agencies to clarify how its standards can be used and that it would develop guidance to help agencies make the most effective use of resources available for physical security across their portfolios of facilities. DHS also provided technical clarifications, which we incorporated as appropriate. Further, DHS said that it concurred with the e-supplement. DOE and USPS did not provide formal written comments on the draft report or e-supplement, but provided technical clarifications, which we incorporated as appropriate. VA, FCC, and OPM did not have any comments on the draft report or e-supplement.

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 to the appropriate congressional committees; the Secretaries of Homeland Security, Energy, and Veterans Affairs; the Postmaster General; the Chairman of the Federal Communications Commission; and the Director of the Office of Personnel Management. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-2834 or GoldsteinM@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on

[39]The second recommendation of the draft report directed the ISC to examine the use of management practices for resource allocation purposes which, among other things, could include compiling and disseminating best practices on such practices. To make the recommendation clearer, we amended it to direct ISC to develop and disseminate guidance on management practices for resource allocation as a supplement to ISC's existing standards. The intent and purpose of the recommendation remained unchanged. We provided the amended recommendation to each of the agencies for comment.

the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely yours,

Mark Goldstein
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to examine (1) the sources that inform how federal agencies conduct their physical security programs and (2) the management practices that agencies use to oversee physical security activities and allocate physical security resources. Our review focused on executive branch agencies that have facilities that are not protected by the Federal Protective Service (FPS) and that have facilities located in the United States and its territories. Facilities in the judicial or legislative branches, military facilities, and facilities located abroad were not included in the scope of our review.

To help inform our research, we reviewed and synthesized reports and documentation on physical security, and interviewed officials familiar with this issue area. For example, we reviewed prior reports from GAO, the Congressional Research Service, and the Congressional Budget Office on the security of federal government facilities and effective program management, as well as documentation from the Department of Homeland Security's Interagency Security Committee (ISC), including physical security standards developed by the ISC. We also interviewed physical security officials at the General Services Administration (GSA); ISC; the Department of Defense (DOD); the Department of State; and ASIS International, an organization for security professionals in the public and private sector that has developed physical security standards for the federal government and non-government entities.[1]

We conducted a web-based survey of 36 cabinet level and independent agencies in the federal government. The surveyed agencies included all non-military agencies that are required under Executive Order 13327 to report to GSA's Federal Real Property Profile (FRPP)[2] as well as those that are not required to report to the FRPP but optionally did so in fiscal year 2010. In addition, although not included in the FRPP, we surveyed the U.S. Postal Service (USPS) because of its large number of federal real property holdings. See appendix II for a list of agencies we surveyed. We obtained responses from all 36 surveyed agencies. To determine whether the surveyed agencies were within the scope of our review, we

[1]Upon interviewing DOD officials, we determined that DOD facilities were not in the scope of our review, which focused on non-military facilities.

[2]FRPP is a centralized real property database maintained by GSA. The FRPP contains data on the federal government's real property inventory, such as what agencies use their buildings for and how many are owned versus leased.

asked questions in the survey to determine if all of their facilities were protected by FPS. Four agencies reported that all of their facilities were protected by FPS, and we therefore did not include them in our review. The remaining 32 agencies are included in our review, and in this report we identify these agencies as the agencies we surveyed. Of the 32 agencies that were within the scope of our review, 16 are primary ISC members, 9 are associate ISC members, and 7 are not members of ISC.[3]

We asked chief security officers or equivalents at the surveyed agencies a series of questions with both closed- and open-ended responses regarding physical security within their agency. The survey included questions on (1) the organization and administration of their agencies, (2) sources used to inform physical security programs, (3) security program policy elements and implementation, (4) challenges and best practices in physical security, and (5) the agencies' building portfolios. We developed the survey questions based on previous GAO work and interviews with agency officials. This report presents survey results in aggregate and does not discuss individual agency responses in a way that would identify them. Summary results for each survey question, except those requiring narrative responses, are available in a supplement to this report, GAO-13-223SP.

Because this was not a sample survey, it had no sampling errors. However, the practical difficulties of conducting any survey can introduce non-sampling errors, such as difficulties interpreting a particular question, which can introduce unwanted variability into the survey results. We took steps to minimize non-sampling errors by pre-testing the questionnaire in person with six different agencies. The agencies were GAO, USPS, the Department of Energy (DOE), ISC, GSA, and the Federal Communications Commission (FCC). We conducted pretests to help ensure that the questions were clear and unbiased, that the data and information were readily obtainable, and that the questionnaire did not place an undue burden on respondents. An independent reviewer within GAO also reviewed a draft of the questionnaire prior to its administration. We made appropriate revisions to the content and format of the questionnaire based on the pretests and independent review.

[3]Membership in the ISC consists of 51 federal agencies and departments, 21 of which are categorized as primary members and 30 of which are associate members. The primary member agencies vote to approve ISC standards; associate members do not vote.

The web-based survey was administered from May 15, 2012, to June 27, 2012. Respondents were sent an email invitation to complete the survey on a GAO web server using a unique username and password. To increase the response rate, we followed up with emails and personal phone calls to respondents to encourage participation in our survey. We then analyzed results of the survey, and as part of this survey analysis, we recoded certain responses that were inconsistent. We followed up with individual agencies as needed to ensure we properly understood what needed to be recoded. All data analysis programs were independently verified for accuracy.

In addition to the survey, we also conducted case studies with five agencies for more in-depth analysis. These case-study agencies were selected to achieve diversity in total building square footage and levels of public access allowed at facilities. The five agencies we selected for our case studies were DOE, the Department of Veterans Affairs (VA), USPS, FCC, and the U.S. Office of Personnel Management (OPM). Based on our review of agency square footage as presented in the Federal Real Property Council's FY2010 Federal Real Property Report, we classified DOE, VA, and USPS as large property holders, and FCC and OPM as small property holders.[4] To ensure that we had diversity in levels of public access at agencies' facilities, we reviewed previous GAO reports and agency websites. For example, from initial interviews, we found that USPS provides a high level of public access to customers where as DOE provides limited public access except for employees and contractors. For each of these five agencies, we interviewed officials in their headquarters offices who are familiar with physical security policy and reviewed documentation on physical security. This report discusses the results of interviews on an individual agency basis, in which case the agency referred to is identified by name, as well as in the aggregate. Since these

[4]Federal Real Property Council, *FY2010 Federal Real Property Report*. The FY2010 report was the most recent report available during our review. The Federal Real Property Council's report provides summary-level information on government-wide real property data, as submitted by federal agencies to the FRPP. GAO has conducted previous work on the reliability of FRPP data, and has found problems with FRPP data collection practices. See GAO, *Federal Real Property: National Strategy and Better Data Needed to Improve Management of Excess and Underutilized Property*, GAO-12-645 (Washington, D.C.: June 20, 2012). However, we found the FRPP data to be reliable for the purposes of selecting which agencies to focus on for our review and to provide a broad overview of the makeup of the government's federal real property portfolio.

agencies were selected as part of a non-probability sample, the findings from our case studies cannot be generalized to all federal agencies.

To supplement these interviews, we conducted site visits to individual DOE, VA, and USPS facilities. For each of these agencies we visited facilities in New Jersey, West Virginia, and Illinois. We selected these locations and facilities to achieve diversity in geographic area, urban and rural environments, and facility risk level as determined by the agencies. We determined which facilities to visit at each location based on FRPP data for DOE and VA, USPS's internal real property database, recommendations from agency officials, and research on the agencies' facilities from their agency websites.[5] The facilities we visited in each state are listed below.

Illinois

- Argonne National Laboratory, DOE, Argonne
- Jesse Brown VA Medical Center, Chicago
- Cardiss Collins Processing and Distribution Center, USPS, Chicago

New Jersey

- Princeton Plasma Physics Laboratory, DOE, Princeton
- Lyons VA Medical Center, Lyons
- Trenton Main Post Office, USPS, Trenton

West Virginia

- National Energy Technology Laboratory, DOE, Morgantown
- Louis A. Johnson VA Medical Center, Clarksburg
- Clarksburg Processing and Distribution Facility, USPS, Clarksburg

At each of these facilities we interviewed facility officials in charge of physical security and reviewed documentation related to physical security. If needed, we also interviewed officials from component offices—which are subordinate entities within an agency, such as bureaus, administrations, and other operating divisions within an

[5]We believe the FRPP and USPS data were sufficiently reliable for the purposes of selecting which facilities to visit.

agency—who oversee facilities with regard to physical security. This report discusses the results of site visit interviews on an individual basis, in which case the agency referred to is identified by name, as well as in the aggregate. Since these facilities and component offices were selected as part of a non-probability sample, the findings from our facility visits cannot be generalized to all federal agencies.

We conducted this performance audit from November 2011 to January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: List of Agencies Surveyed

We conducted a web-based survey of 36 cabinet level and independent agencies. These 36 agencies are those non-military agencies that are required under Executive Order 13327 to report to the Federal Real Property Profile (FRPP);[1] those that voluntarily reported to the FRPP in 2010; and the U.S. Postal Service which, although not included in the FRPP, is one of the federal government's largest real property holders. The agencies we surveyed are listed below. Four agencies reported that all of their facilities were protected by FPS, and we therefore did not include them in our review.

American Battle Monument Commission
Broadcasting Board of Governors
Court Services and Offender Supervision Agency
Department of Agriculture
Department of Commerce
Department of Education
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of Treasury
Department of Veterans Affairs
Environmental Protection Agency
Federal Communications Commission
General Services Administration
John F. Kennedy Center for Performing Arts
Merit Systems Protection Board
National Aeronautics and Space Administration
National Archives and Records Administration
National Gallery of Art
National Science Foundation

[1]The FRPP is a centralized real property database maintained by the General Services Administration. The FRPP contains data on the federal government's real property inventory, such as what agencies use their buildings for and how many are owned versus leased.

Nuclear Regulatory Commission
U.S. Office of Personnel Management
Peace Corps
Small Business Administration
Smithsonian Institution
Social Security Administration
Tennessee Valley Authority
U.S. Postal Service
United States Agency for International Development
United States Holocaust Memorial Council

Appendix III: Comments from the Department of Homeland Security

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

Homeland Security

January 17, 2013

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

Re: Draft Report GAO-13-222, "FEDERAL FACILITY SECURITY: Greater Outreach by DHS on Standards and Management Practices Could Benefit Agencies"

Dear Mr. Goldstein:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note how this report highlights the essential role the Interagency Security Committee (ISC) plays in informing physical security standards. As stated in the report, ISC standards, which are developed on the basis of leading security practices across the Government, set forth a decision-making process to help ensure agencies have effective physical security programs in place. The ISC 2012–2017 action plan also cited in the report contains an initiative that supports the establishment of protocols and processes for monitoring and testing compliance with its standards, which could include agency self-assessments or ISC officials assessing agency compliance.

The draft report contained two recommendations with which DHS concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct the ISC:

Recommendation 1: To help achieve the purpose of Executive Order 12977 to enhance the quality and effectiveness of security of Federal facilities, conduct outreach to all executive branch agencies to clarify how the standards can be used in concert with agencies' existing physical security programs.

Response: Concur. The ISC currently conducts outreach through annual member meetings, quarterly meetings, and working groups or subcommittee meetings. The ISC will review current outreach efforts to determine the best way these efforts can be expanded with current funding and to clarify how the standards can be used in concert with agencies' existing physical security programs, as needed, in accordance with Executive Order 12977.

Recommendation 2: To help agencies make the most effective use of resources available for physical security across their portfolio of facilities, examine the use of management practices for

resource allocation purposes. This examination could include identifying practices most beneficial for physical security programs, determining the extent to which federal agencies currently use these practices, and compiling and disseminating best practices that agencies could use on a voluntary basis.

Response: Concur. The ISC standards set forth a decision-making process to help ensure that agencies have effective physical security programs in place. We will remain diligent in the continuous improvement of physical security programs going forward. As a supplement to the ISC's existing physical security standards; the ISC will develop guidance to help agencies make the most effective use of resources available for physical security across their portfolio of facilities and examine the use of management practices for resource allocation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

2

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Heather Halliwell (Assistant Director), Eli Albagli, Steve Caldwell, Roshni Davé, Colin Fallon, Kathleen Gilhooly, Jill Lacey, Hannah Laufe, Ying Long, Sara Ann Moessbauer, John Mortin, and Nitin Rao made key contributions to this report.