United States Government Accountability Office

Report to the Ranking Member, House Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives

December 2018

FEDERAL BUILDING SECURITY

Actions Needed to Help Achieve Vision for Secure, Interoperable Physical Access Control

Accessible Version

GAO-19-138

December 2018

FEDERAL BUILDING SECURITY

Actions Needed to Help Achieve Vision for Secure, Interoperable Physical Access Control

GAO Highlights

Highlights of GAO-19-138, a report to the Ranking Member, Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representative

Why GAO Did This Study

A 2004 federal directive and the related standard set forth a vision for using information technology to verify the identity of individuals accessing federal buildings. The vision calls for secure and reliable forms of identification that work in conjunction with access control systems. Interoperability of these systems across departments and agencies is part of the vision. OMB and GSA have government-wide responsibilities related to this effort. ISC provides guidance to non-military executive branch agencies on physical security issues. GAO was asked to examine PACS implementation efforts.

This report discusses (1) steps OMB and GSA have taken to fulfill their government-wide responsibilities related to PACS and (2) challenges selected federal agencies face in meeting current requirements. For review, GAO analyzed documents from Commerce, GSA, ISC, and OMB. GAO selected five non-military agencies based on factors including number of buildings and geographic location. GAO reviewed relevant requirements and key practices. GAO also interviewed federal agency officials, PACS vendors, and knowledgeable industry officials.

What GAO Recommends

GAO recommends (1) that OMB determine and regularly monitor a baseline level of progress on PACS implementation and (2) that ISC assess the extent of, and develop strategies to address, government-wide challenges to implementing PACS. OMB had no comment on the recommendation. DHS concurred with the recommendation to ISC.

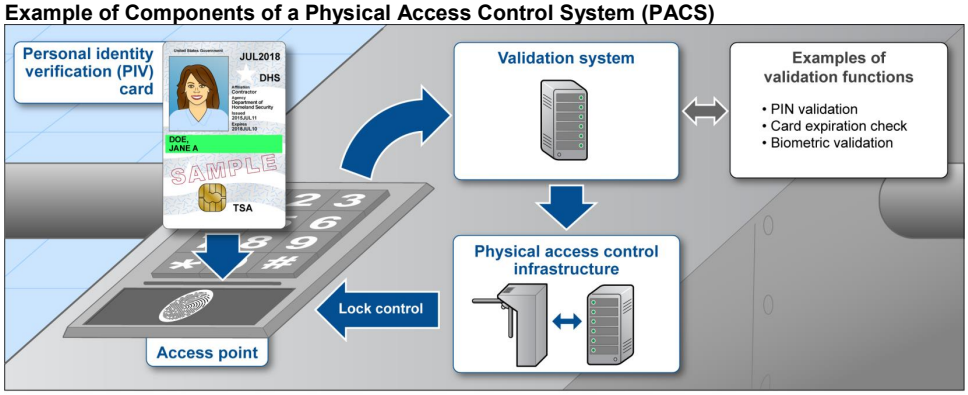
View GAO-19-138. For more information, contact Lori Rectanus at (202) 512-2834 or rectanusl@gao.gov.

What GAO Found

The Office of Management and Budget (OMB) and the General Services Administration (GSA) have taken steps to help agencies procure and implement secure, interoperable, GSA-approved "physical access control systems" (PACS) for federal buildings. PACS are systems for managing access to controlled areas within buildings. PACS include identification cards, card readers, and other technology that electronically confirm employees' and contractors' identities and validate their access to facilities (see figure). Steps taken include the following:

- OMB issued several memos to clarify agencies' responsibilities. For example, OMB issued a 2011 memo citing Department of Homeland Security (DHS) guidance that agencies must upgrade existing PACS to use identity credentials before using relevant funds for other activities. But, GAO found OMB's oversight efforts are hampered because it lacks baseline data on agencies' implementation of PACS. Without such data, OMB cannot meet its responsibility to ensure agencies adhere to PACS requirements or track progress in implementing federal PACS requirements and achieving the vision of secure, interoperable systems across agencies.
- GSA developed an Approved Products List that identifies products that meet federal requirements through a testing and evaluation program. Federal agencies are required to use the Approved Products List to procure PACS equipment. GSA also has provided procurement guidance to agencies through its identity management website.

Example of Components of a Physical Access Control System (PACS)



Source: GAO. | GAO-19-138

Officials from the five selected agencies that GAO reviewed identified a number of challenges relating to PACS implementation including cost, lack of clarity on how to procure equipment, and difficulty adding new PACS equipment to legacy systems. Officials from OMB, GSA, and industry not only confirmed that these challenges exist but also told GAO that they were most likely present across the federal government. The Interagency Security Committee (ISC), chaired by the DHS and consisting of 60 federal departments and agencies, has a mission to develop security standards for non-military agencies. In this capacity the ISC is well-positioned to determine the extent that PACS implementation challenges exist across its membership and to develop strategies to address them. An ISC official told GAO that the ISC has taken steps to do so including setting up a working group to assess what additional PACS guidance would be beneficial.

Contents

Figures

Abbreviations

DHS	Department of Homeland Security
EPA	Environmental Protection Agency
E-PACS	Enterprise Physical Access Control System
FIPS	Federal Information Processing Standards
GSA	General Services Administration
GSA Schedules	GSA's Federal Supply Schedules program
HSPD-12	Homeland Security Presidential Directive 12

ISC	Interagency Security Committee
NIST	National Institute of Standards and Technology
OGP	Office of Government-wide Policy
OMB	Office of Management and Budget
PIN	personal identification number
PIV	personal identity verification
TSA	Transportation Security Agency

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 20, 2018

The Honorable J. Luis Correa
Ranking Member
Subcommittee on Oversight and Management Efficiency
Committee on Homeland Security
House of Representatives

Dear Mr. Correa:

In an effort to increase the security of federal facilities and information systems where there is potential for terrorist attacks such as those that occurred on September 11, 2001, Homeland Security Presidential Directive 12 (HSPD-12) established the requirement for a mandatory, government-wide identification standard for federal government employees and contractor personnel in August 2004. The standard specifies the technical requirements for physical access control systems to issue secure and reliable identification credentials to federal employees and contractors for gaining access to federal facilities and information systems. In order to meet this standard, agencies have begun implementing enhanced physical access control systems for controlling employees' and contractors' access to buildings. These systems use personal identity verification (PIV) cards that operate with networked physical access control systems, so that agencies can make sure that the employees and contractors who enter federal buildings are who they claim to be and have the proper authority to enter. To implement this vision and in response to HSPD-12, standards and guidance also call for the interoperability of these systems across agencies."[1]

Several federal agencies have key government-wide responsibilities for this effort. The Office of Management and Budget (OMB) is responsible

[1] According to the General Services Administration and its testing contractor, in order for this certificate authentication process to be successful, physical access control system equipment must be networked so that physical access control systems can communicate with directories maintained by issuers of cards; physical access control systems that are not networked will lack access to this extra level of security. A networked physical access control system can confirm not only the validity of a credential's issuer, but also the authenticity and validity of any given credential. This validity must be confirmed with the card's issuer every 18 hours; otherwise, a physical access control system must deny access.

for the program's overall direction and oversight. The General Services Administration (GSA) is responsible for testing physical access control systems to ensure they meet security and interoperability standards and identifying such systems through its Approved Products List. OMB and the Federal Acquisition Regulation require agencies to use the Approved Products List when buying physical access control systems to achieve an integrated approach to physical security.[2] The Interagency Security Committee (ISC), chaired by the Department of Homeland Security (DHS), plays a key role in ensuring the protection of nondefense buildings and facilities and security for them in the United States. The Department of Commerce's National Institute of Standards and Technology (NIST) sets technical specifications that form the basis of standards, including for example, the minimum requirements for a federal PIV system that meets the control and security objectives of HSPD -12.[3]

Implementation of physical access control systems at federal agencies represents a significant federal investment. For example, over the next 5 years, TSA plans to spend about $73 million to implement physical access control systems with the bulk of these funds ($51 million) going toward the acquisition of new systems from the Approved Products List. TSA is one of hundreds of federal agencies. In addition, according to GSA officials, GSA has spent millions of dollars to test these systems. However, a congressional committee and some industry stakeholders have raised questions about the implementation of this directive, specifically about the extent to which agencies are using the Approved Products List to purchase physical access control systems. Not only could purchasing products not on the Approved Products List lead to wasteful spending, but such purchases could result in security breaches if, for example, elements of access credentials are counterfeited, cloned, or copied, and physical access control systems fail to detect them.

In support of congressional oversight of federal buildings' security, you asked that we examine issues related to agencies' implementation of

[2] The Federal Acquisition Regulation generally governs the acquisition of goods and services by executive branch agencies. It addresses various aspects of the acquisition process from acquisition planning to contract management.

[3] *NIST Special Publication 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, published in November 2008, provides guidelines for the use of PIV cards in physical access control systems. This document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to federal government facilities.

federal physical access control system requirements. Our objectives were to (1) assess steps OMB and GSA have taken to fulfill their government-wide responsibilities related to requirements for implementing physical access control systems and (2) identify challenges selected federal agencies face in meeting requirements for federal physical access control systems.

To address these objectives, we interviewed OMB and GSA about their efforts to fulfill their government-wide responsibilities in this area. We also asked them to provide data on agencies' Approved Products List usage. We interviewed private sector companies that have key roles in government-wide implementation of HSPD-12, specifically: seven manufacturers of physical access control systems, five integrators (contractors who install the equipment and connect it to agency networks with software), as well as other industry organizations, including a trade association, GSA's contractor that tests physical access control systems for the Approved Products List, and a long-time industry consultant.

To identify illustrative examples of the progress that individual agencies have made in using the Approved Products List to implement HSPD-12 requirements, as well as the challenges that they have faced in doing so, we selected five executive branch agencies: (1) the U.S. Coast Guard in DHS; (2) the Bureau of Prisons in the Department of Justice (Justice); (3) the Transportation Security Agency (TSA) in DHS; (4) the Environmental Protection Agency (EPA); and (5) the General Services Administration. Our criteria for agency selection included, but were not limited to, agencies with facilities (1) held by non-defense executive branch agencies; (2) located in the United States; and (3) totaling 200 or more buildings. We limited our scope to non-defense agencies because we also have other ongoing work related to these issues at the Department of Defense. We interviewed knowledgeable officials at these agencies about the Approved Products List and reviewed information on agencies' purchases of GSA-approved physical access control systems equipment using the Approved Products List since 2013, the year GSA began conducting more rigorous testing and approval of physical access control system equipment. Our use of the term stakeholders in this report may refer to agencies, physical access control manufacturers, integrators, and knowledgeable organizations or officials. Results from our interviews with the selected agencies cannot be generalized. To identify challenges selected federal agencies face in adhering to federal physical access control system requirements, we reviewed relevant trade industry literature and conducted an analysis of our interviews with agency officials. In addition to considering the range of federal requirements

related to physical access control, we evaluated agency activities related to monitoring and oversight against pertinent standards for internal controls in the federal government and leading practices for collaboration identified in prior GAO work.[4] See Appendix I for more detail about our methodology.

We conducted this performance audit from October 2017 to December 2018 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.

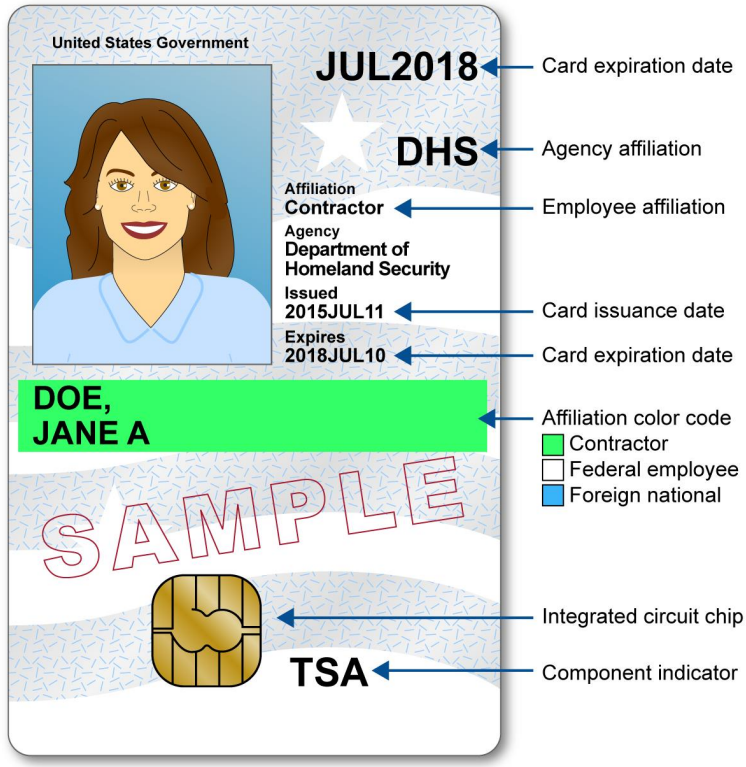
Background

Personal Identity Verification Cards

Developed in response to HSPD-12, Personal Identity Verification (PIV) cards are a common authentication mechanism used across the federal government, and are a component of physical access control systems. PIV cards are used to securely identify federal government employees and contractor personnel seeking access to valuable and sensitive federal resources, including facilities and information systems. Also known as a “smart card,” a PIV card is similar in size to a credit card and contains information that is either printed on the outside or stored on the card’s integrated circuit chip (see fig. 1 below). PIV cards are required to be interoperable with all GSA-approved physical access control system equipment included on the Approved Products List, regardless of that equipment’s manufacturer. Likewise, GSA-approved physical access control system equipment is required to be interoperable with all PIV cards.

[4] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G, (Washington, D.C.: September 2014); GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

Figure 1: Key Information on a Sample Personal Identity Verification (PIV) Card



Source: GAO. | GAO-19-138

Access to Controlled Areas

Physical access control systems are used to manage access to controlled areas, such as a building or a room in a building. Physical access control products include devices such as card readers and the ID cards used to validate an individual's authorization to enter a building (see fig.2 below). This report focuses on physical access and does not address logical (computer network) access.[5]

A physical access control system works as follows. When employees or contractors who are PIV cardholders attempt to enter a controlled area

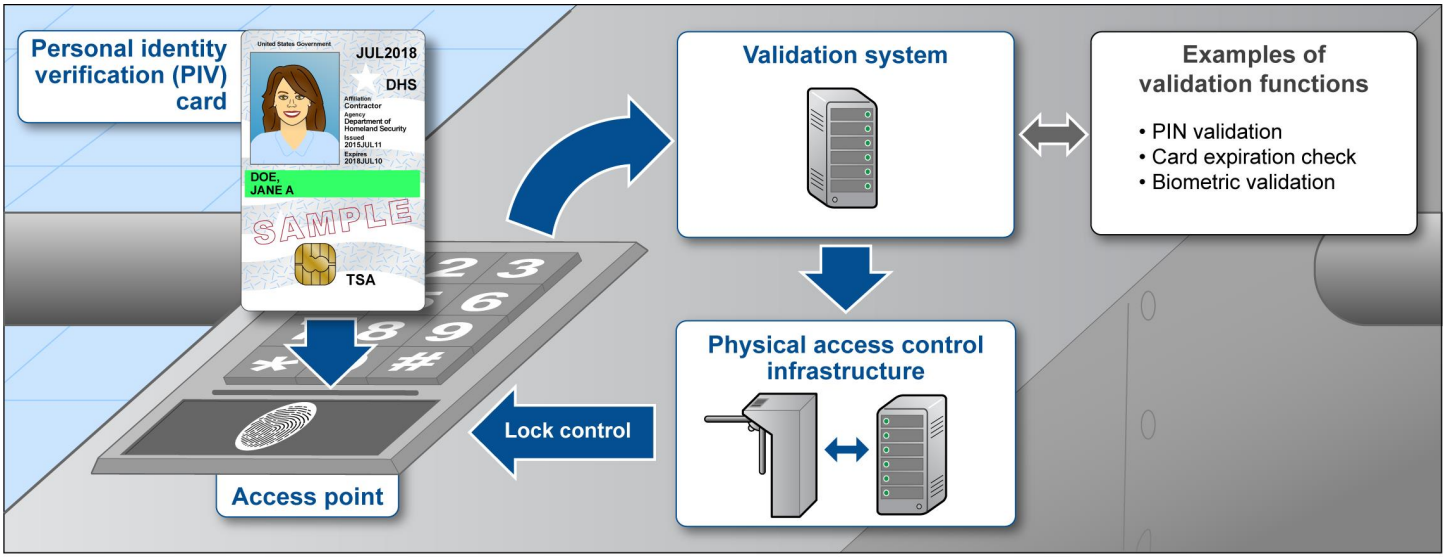
[5] Physical access refers to entry to a secured building, wing, floor, or room that a PIV cardholder wishes to enter. In contrast, logical access is typically entry to a network or a location on a network (e.g., a computer workstation, folder, file, database record, or software program).

managed by a physical access control system, they will encounter the physical access control system at the "front end." At this point, depending on the controlled area's level of security, the cardholder will

- scan their PIV cards via a card reader,
- insert their PIV cards and enter personal identification numbers (PIN) via an input device such as a keypad, or
- insert their PIV cards, enter PINs, and provide biometric identification (such as a fingerprint) via an input device.

After the cardholders present their identification information, the cardholders' identification information from a PIV card's integrated circuit chip is transmitted to the physical access control system's "back end," which consists of physical and logical access control systems and authorization data. At the back end, the physical access control system determines the validity of the cardholder's access authorization. The cardholder will be able to access the area only if the authorization is valid.

Figure 2: Example of Components of a Physical Access Control System



Source: GAO. | GAO-19-138

When deciding which access control mechanisms to implement, agencies must first understand the level of risk associated with the facility. The higher the risk level, the greater the need there is for agencies to implement a high-assurance-level access control system. Physical access control systems can be electronically connected in different ways, including within a given building or across an agency or department. The

level of interoperability determines the level at which PIV cards and access authorization will be accepted. For example, a PIV card and corresponding access authorization may be accepted within a single building, across an agency, or potentially across the federal government. In this report, we describe a system in which a PIV card works in multiple physical access control systems as "interoperable". In order to realize the full security benefit of PIV cards, physical access control systems must have a network connection that enables them to validate a given cardholder's access credentials.[6]

Federal Requirements

Homeland Security Protection Directive-12: HSPD-12 is a 2004 presidential directive establishing the requirement for a mandatory, government-wide standard for secure and reliable forms of identification (PIV cards) issued by the federal government to its employees and contractors. It specified that the standard must include criteria authenticating employees' identities and permissions at graduated levels of security, depending on the agency environment and the sensitivity of facilities and data accessed.

Federal Information Processing Standards (FIPS) 201: The Department of Commerce's NIST initially published the Federal Information Processing Standards (FIPS) 201 in 2005 to support HSPD-12. The FIPS 201 standard established the PIV card as a common authentication mechanism across the federal government. FIPS 201 set standards for PIV systems in three areas: (1) identity proofing and registration, (2) card issuance and maintenance, and (3) protection of card applicants' privacy. In addition, the standard provides technical specifications for the implementation and use of interoperable smart cards in physical access control systems. An update to FIPS 201 (called FIPS 201-2), was released in August 2013. Among other things, it made the collection of a facial image mandatory for PIV cards and changed the maximum lifespan of a card from 5 to 6 years.

[6] A GSA official told us that this process is analogous to the use of credit cards: when a credit card's holder makes a purchase at a store, the cash register must be networked in order to confirm that the cardholder has sufficient available credit. Similarly, a physical access control system uses a network connection to validate the cardholder's access credentials.

Approved Products List – The Approved Products List is a list of all physical access control system equipment that is compliant with FIPS identification standards. Agencies must acquire federally-approved products and services from this list in order to help ensure government-wide interoperability of physical access control systems.[7] All products on the Approved Product List have gone through end-to-end testing and evaluation, as part of a complete physical access control system.[8] Federal agencies are required to use the Approved Products List when purchasing physical access control system equipment. The Approved Products List is intended to provide assurance to federal agencies that listed vendors' products comply with the various federal standards and requirements.[9]

Government-wide Roles and Responsibilities

Office of Management and Budget (OMB)

HSPD-12 designates OMB as the lead entity with responsibility for ensuring that federal government departments and agencies implement this directive in a manner consistent with ongoing government-wide activities and existing OMB policies and guidance.

General Services Administration (GSA)

GSA supports OMB by administering product testing through a contractor, managing the Approved Products List, and making the physical access control system's products and services available to federal agencies via

[7] OMB, *Memorandum for the Heads of All Departments and Agencies: Implementation of Homeland Security Protection Directive 12 (HSPD-12 - Policy for a Common Identification Standard for Federal Employees and Contractors*, M-05-24 (Washington, D.C.: Aug. 5, 2005).

[8] End-to-end testing is a methodology used to test whether a system is performing as it will be implemented in actual usage.

[9] Stakeholders told us that, after the issuance of HSPD-12 in 2004, physical access control systems products initially were approved for the Approved Products List through self-testing undertaken by manufacturers. However, this approach was used to test products individually rather than as systems. Partly as a result, agencies encountered functionality issues when deploying the equipment as part of a physical access control system. In 2013, GSA changed the process for getting products on the Approved Products List, requiring that equipment be tested as part of end-to-end systems, and engaged a contractor for this purpose. According to stakeholders and federal officials, functionality issues have been significantly reduced.

GSA's Federal Acquisition Service. The Federal Acquisition Service manages a large portion of GSA's Federal Supply Schedules program (GSA Schedule), which establish long-term government-wide contracts with commercial firms to provide federal agencies access to millions of commercial products and services at volume discount pricing. [10] Further, GSA's Office of Government-wide Policy (OGP) provides tools and support for identity, credential, and access management activities across the federal government, including for physical access control systems. GSA also has a government-wide landlord role through its Public Buildings Service and installs physical access control systems in many GSA-owned and leased buildings that it manages.[11]

Interagency Security Committee

The ISC is chaired by DHS and consists of 60 federal departments and agencies. ISC's mission is to develop security standards, best practices, and guidelines for nonmilitary federal facilities in the United States. Each of the five selected agencies included in our report, or their home departments, is a member of the ISC. The ISC has the authority to convene working groups from its member agencies to produce documents, which are task-based and provide ISC's members with a forum for information sharing to address a wide range of issues related to physical security at federal buildings. ISC also produces standards and best practices guidance for agencies to use when addressing security issues. For example, in December 2015 ISC released *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide*. This document is intended to identify practices most beneficial for physical security programs, determine the extent to which federal agencies currently use these practices, and compile and circulate best practices agencies can use as a supplement to the ISC's existing security standards.

[10] While GSA establishes prices associated with volume buying, agencies are generally required to further compete their specific requirements among Schedule contractors and seek further discounts. Different Schedules are generally used to purchase different categories of goods and services. For example, GSA Schedule 70 is generally used for information technology purchases, while GSA Schedule 84 is generally used for physical security equipment purchases.

[11] According to representatives of GSA, there may be some circumstances in which its Public Buildings Services is not responsible for implementing physical access control systems in some properties.

OMB and GSA Have Taken Steps to Fulfill Their Responsibilities to Implement Physical Access Control Systems, but Oversight Is Limited

OMB and GSA Have Supported Implementing Physical Access Control Systems

OMB and GSA have taken steps to help agencies procure and implement secure and interoperable GSA-approved physical access control systems across the federal government. For example, OMB has issued three guidance memorandums to clarify agency responsibility to use GSA's Approved Products List.

1. In 2005, OMB designated GSA as the "executive agent for government-wide acquisitions of information technology" for the products and services required for physical access control and delineated agency responsibilities with regard to implementing HSPD-12.[12] Also, to ensure government-wide interoperability, all agencies must acquire products and services that are compliant with standards and included on the Approved Products List.
2. In 2006, OMB reiterated that agencies must purchase physical access control systems from GSA's Approved Products List and that GSA will make approved products and services available through acquisition vehicles (Schedules) that are available to federal agencies.[13]
3. In 2011 OMB issued a memo that cited DHS guidance that stated effective in fiscal year 2012 agencies must upgrade existing physical and logical access control systems to use PIV credentials prior to

[12] OMB memo M-05-24.

[13] OMB, Memorandum for Chief Information Officers, Chief Acquisition Officers, Chief Financial Officers: Acquisition of Products and Services for Implementation of HSPD-12, M-06-18, (Washington, D.C.: June 30, 2006).

using relevant funds for other activities.[14] The memorandum further stated that the upgrades must be in accordance with NIST standards.

In addition, GSA, as the lead agency for government-wide acquisition of information technology, has undertaken a number of efforts to promote the implementation of GSA-approved physical access control systems:

1) **Testing and evaluation:** GSA administers and conducts testing and evaluation to develop an Approved Products List. Testing is performed by either third-party accredited testing labs or GSA-managed testing labs. GSA tests a variety of products and services including smart cards; physical access control systems; which include card readers and infrastructure for example; and integrators which provide or install access control services. According to GSA officials, GSA has fully tested all physical access control system equipment included on the Approved Products List and evaluated and approved the suitability of vendors and system integrators. GSA shares information about vendors, system integrators and Approved Products List equipment with federal agencies.

2) **Guidance and support:** GSA has taken several actions to improve guidance and facilitate the implementation of physical access control systems. First, GSA manages IDManagement.gov, which guides federal agencies through the process of identifying Approved Products List-compliant physical access control system equipment. Second, GSA established the U.S. Access program to enable federal civilian agencies to issue common HSPD-12 approved credentials to their employees and contractors. Finally, GSA developed a list of system integrators that can be used to install physical access control systems that have been approved for the Approved Products List. These integrators (there are 25 as of November 2018) are listed on the GSA's IDManagement.gov website.

3) **Information sharing:** According to GSA officials, GSA responds to email questions from agencies about the Approved Products List, and GSA makes subject matter experts available to any agency representatives with questions.

[14] OMB, Memorandum for the Heads of Executive Departments and Agencies: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors, M-11-11 (Washington, D.C.: Feb. 3, 2011).

4) **Procurement support:** According to GSA officials, GSA provides standard procurement language for agencies to include in statements of work before their requests for proposal go out for physical access control systems. However, according to officials, GSA has no control over whether agencies decide to include the language that it provides.

Stakeholders including agencies and manufacturers that we interviewed generally considered the Approved Products List to have achieved its intent. For example, government and industry officials said that they believe the list provides assurance to government agencies that physical access control systems will work as intended and will help facilitate a more interoperable system government-wide, thereby enhancing security. Moreover, stakeholders we interviewed said they generally thought the associated costs and burdens of going through GSA's testing and evaluation have been worth the effort. Without the Approved Products List, these stakeholders believe that the quality and interoperability of products would diminish. According to some stakeholders, prior to the current end-to-end testing of products, companies submitted products to the Approved Products List that either did not work as intended or were not compatible with other products. Stakeholders also commented on the improvements to the Approved Products List since GSA took over the certification testing, noting that use of manufacturer self-testing prior to 2012 was not successful. In addition, the cost to industry to do self-testing was high, according to vendors, and some companies did not do it well, according to GSA, EPA, and TSA officials.[15]

OMB Lacks Necessary Information to Conduct Oversight

We found that neither OMB nor GSA currently collect data on agency efforts to implement physical access control system requirements, including use of the Approved Products List. This is significant because our interviews with physical access control systems' manufacturers, integrators, and selected agencies indicate that government-wide implementation of physical access control systems may be limited and raises questions about government-wide progress. Officials from four of the five selected agencies we reviewed told us that, since 2013, when physical access control system end-to-end testing requirements began,

[15] OMB officials told us that the manufacturer self-testing that occurred from 2005-2013 involved a process that included specific testing criteria and National Institute of Standards and Technology-certified labs. These officials said that while this testing approach did face challenges, it evolved over time.

they had only purchased GSA-approved physical access control system equipment for a limited number of their facilities. Moreover, they said that where purchasing occurred, it was sometimes for physical access control systems that required replacement because they were nearing the end of their useful life.[16]

For the five selected agencies, we found the following:

- **General Services Administration:** According to GSA officials, a limited number of GSA facilities have physical access control systems that fully adhere to the latest requirements.[17] According to GSA officials, GSA has met federal physical access control system requirements for 70 out of approximately 340 of its non-courthouse buildings with another 90 being partially in line with requirements (e.g., PIV access credentials are used). The remaining facilities do not yet meet federal physical access control system requirements. GSA staff also told us that GSA administers the public spaces in approximately 360 courthouse buildings and is developing a security implementation plan for these spaces. GSA officials told us that GSA also administers about 8,000 leased buildings where the tenants in these spaces are generally responsible for setting up physical access control systems and GSA does not track this information.
- **Environmental Protection Agency:** According to EPA officials, none of EPA's 72 facilities (including, for example, its headquarters building in the District of Columbia and 10 regional headquarters buildings) currently adhere to the latest physical access control system requirements. Specifically, EPA officials told us that the agency used GSA's Approved Products List to purchase physical access control system equipment in the past. However, because requirements have changed over time, the 72 buildings where EPA is responsible for physical access control need to be upgraded to the latest

[16] Agencies' officials told us that physical access control systems are not required in all areas of federal buildings. Risk assessments, as recommended by ISC guidance, should determine where physical access control systems are necessary.

[17] According to GSA officials, GSA is responsible for physical access control at about 700 buildings managed by GSA's Public Buildings Service, including 340 non-courthouse buildings.

requirements.[18] To do so, EPA officials said they will procure these systems using the Approved Products List and prioritize implementation in the future to those facilities with the highest assessed risk. EPA officials said that in August 2013, changes to physical access control systems' standards required the agency to purchase and install complete physical access control systems that GSA has tested end-to-end and that adhere to the latest requirements. EPA officials said they expect the end-to-end tested physical access control systems to lead to systems that are more secure and interoperable.

- **Bureau of Prisons:** The Bureau of Prisons has implemented Approved Products List-compliant physical access control system equipment in regional and central offices according to agency officials we interviewed. According to officials, the Bureau of Prisons purchased physical access control systems using the Approved Products List for its headquarters complex (three buildings) and six regional offices beginning in 2009 and made upgrades to this equipment in 2015 to adhere to federal physical access control system requirements at the time. However, Bureau of Prisons officials told us that the agency has not implemented physical access control systems at its institutions (prisons). Bureau of Prisons officials told us that physical security and screening procedures at prisons are more stringent than those that occur with typical building-access procedures as persons and belongings are scanned and searched. Physical access control system equipment at these prisons may in fact be problematic because, according to Bureau of Prisons officials, doors should not automatically be opened based on a PIV card without manual checks to ensure staff are not under duress or fraudulent access is being attempted. Bureau of Prisons officials said that at the prisons, identification credentials are first visually examined by prison personnel before access is granted, and all gates and points of entry are controlled by prison personnel.[19]
- **Transportation Security Administration:** According to TSA officials, since 2013, 64 TSA facilities have implemented some physical access

[18] EPA officials told us that all EPA's buildings currently adhere to FIPS 201-1 or FIPS 201-2 requirements, but none of its buildings adheres to the latest Enterprise Physical Access Control System (E-PACS) requirements. E-PACS systems allow federal government personnel and contractors to authenticate their identities as visitors at other agencies using PIV cards already issued by their own agency.

[19] We did not make a determination as to whether the Bureau of Prisons should adhere to physical access control requirements at its prisons.

control system upgrades using products from the Approved Products List, while an additional 75 leased facilities have been upgraded by GSA. While the 139 facilities are not fully compliant, the only item missing to make these facilities compliant, according to TSA officials, is the capability for interoperable, secure identification checks among federal agencies. This would allow TSA's physical access control systems to recognize revoked PIVs from any federal agency. TSA told us that it plans to roll out this capability in fiscal year 2019. Our review of TSA's 2015 plan to meet the latest physical access control system requirements indicates that the agency is taking steps toward full compliance. TSA's implementation plan was developed in response to DHS's 2012 Modernization Strategy for Physical Access Control Systems, which provides guidance to DHS for implementing secure and compliant end-to-end physical access control systems from GSA's Approved Products List. Over the next 5 years, TSA plans to spend about $73 million in physical access control system implementation with the bulk of these funds ($51 million) going toward the acquisition of new systems from the Approved Products List.

- **United States Coast Guard:** Coast Guard officials told us that none of the agency's 1,400 facilities where it has security responsibilities fully adhere to the latest federal physical access control system requirements. However, 53 of these facilities have been prioritized for physical access control system implementation. In addition, since 2013, four Coast Guard locations have begun to implement GSA-approved physical access control systems using the Approved Products List. These locations are Jacksonville, FL; New York, NY; Corpus Christi, TX; and the Coast Guard's Security Center in Chesapeake, VA. Decisions about physical access control system equipment are made on a facility-by-facility basis, according to Coast Guard officials. These officials said that due to the decentralized nature of Coast Guard's decision-making process for physical access control systems, it is difficult to say where purchases have been made, and there is no systematic tracking. The Coast Guard does not have a formal plan for upgrading its physical access control systems, but Coast Guard officials told us that they continue to pursue opportunities to upgrade facilities with physical access control system equipment using the Approved Products List. For example, Coast Guard officials told us that they currently emphasize system upgrades for those systems that reach the end of their useful life or otherwise necessitate replacement.

These five selected agencies are illustrative of the oversight difficulties that OMB faces because it does not have baseline information about agencies' efforts to implement physical access control systems, including

implementation of GSA-approved systems. This lack of information hampers OMB's efforts to (1) meaningfully track and monitor agencies' adherence to physical access control system requirements, or (2) provide an incentive for agencies to be more accountable with regard to where their physical access control systems stand in terms of their ability to prevent security breaches. Federal internal-control standards state that establishing a baseline is an internal control that can be used to perform monitoring activities. Baseline data allow organizations to identify and address performance issues and deficiencies. Establishing a baseline to understand the current status of physical access control system implementation could improve efforts to evaluate progress federal agencies are making and could also provide an incentive to agencies to further improve. Moreover, federal internal-control standards also direct agencies to hold organizations accountable for their assigned responsibilities.

OMB staff said that OMB oversees physical access control systems' requirements as part of its normal process of reviewing agencies' budget submissions but does not conduct oversight outside of this process. This approach, however, does not allow OMB to identify or monitor the extent to which agencies are purchasing physical access control systems that meet the latest requirements or take action if agencies lag in this area.

Selected Agencies Have Faced Various Challenges in Meeting Physical Access Control Systems' Requirements and May Benefit from Additional Government-wide Support

Selected federal agencies face cross-cutting, as well as agency-specific, challenges to acquiring and integrating physical access control system equipment, according to agency representatives and industry stakeholders we spoke to. These challenges include cost, confusion regarding GSA Schedule's use, lack of trained agency officials, adapting legacy systems, and security concerns about integrating physical access control systems.

- **Cost:** Officials from most of the five selected agencies, from physical access control system manufacturers, and from integrators we interviewed told us that the cost of buying GSA-approved physical access control systems using the Approved Products List and

installing them in adherence to federal physical access control system requirements is a challenge in the current budget environment. Agency representatives also told us they view the regulatory and OMB requirement to upgrade physical access control systems as a costly unfunded mandate that these agencies have difficulty meeting. For example, TSA officials estimate that TSA will need over $14 million per year to continue implementing GSA-approved physical access control systems using the Approved Products List in its 625 facilities, an expense for which the agency receives no additional funds. However, OMB staff told us that agencies have had 13 years in which to replace physical access control systems' technology with products that meet federal requirements, and that the issue may be agencies' training and planning, rather than cost. OMB staff told us that the expectation was, that over time, agencies would implement physical access control systems that used equipment that was exclusively from the APL and compliant with FIPS.

- **Confusion regarding GSA Schedules:** Officials from some of the five selected agencies and some stakeholders told us that there is some uncertainty in government and industry about which GSA contracting Schedule should be used to acquire GSA-approved physical access control system equipment and services. For example, some stakeholders are unsure which GSA Schedule they should use to provide their services. GSA Schedule 70 is generally used for information technology purchases.

  GSA Schedule 84 is generally used for physical security equipment purchases, including products such as security alarms and surveillance equipment. However, some stakeholders told us they found federal guidance unclear as to whether Schedule 70 or 84 should be used for GSA-approved physical access control system purchases. For example, some integrators told us that it was not always clear for what Schedule they should seek approval to be on to sell their services.[20] Federal regulations and an OMB memo both mention Schedule 70 as being the appropriate Schedule for purchasing physical access control systems, but do not explicitly exclude the use of Schedule 84.

  Complicating matters, some stakeholders told us some companies are only approved for Schedule 84 because getting approved for both

[20] Service providers must meet certain requirements and be approved to offer their services though a given GSA Schedule.

Schedules was time-consuming and costly, and not worth the effort given the lack of clarity regarding which Schedule is required. According to OMB staff, guidance is clear that Schedule 70 should be used to purchase physical access control equipment because this equipment is considered to be information technology. OMB staff explained that their memo on this subject was not intended to introduce ambiguity on the issue of what Schedule is appropriate for use, but to accommodate practices at the Department of Defense, which performs some of its own product testing separate from GSA's testing program.[21] According to GSA's Office of Government-wide Policy (OGP), GSA is aware of the confusion among GSA's federal customers regarding GSA Schedule use. To address this situation, GSA convened a "reverse industry" training event in September 2018, at which industry representatives provided feedback to GSA on the acquisition process and ways that it could be improved, including issues pertaining to acquisitions related to physical access control systems. According to federal officials, one point of emphasis by industry was that purchasing physical access control equipment from the Approved Products List was not sufficient for having a functioning physical access control system; system integration was also necessary. During this event, GSA officials took the position that both Schedule 70 and Schedule 84 could be used to purchase physical access control systems, but OMB staff maintain that Schedule 70 is preferred. OMB staff explained that Schedule 84 does not have the testing and evaluation requirements for PACS equipment on it that Schedule 70 does. According to OMB, this frustrates industry vendors that follow the Schedule 70 approval process because these vendors are spending time and money to get approved for Schedule 70, while others are still selling their equipment on Schedule 84 and skirting this process because GSA allows the sale of physical access control system equipment on both Schedules. Schedule 84 has historically been used for security hardware while Schedule 70 is used for information technology. Since physical access control systems are essentially information technology systems today, OMB believes that Schedule 70 should be used exclusively for physical access control system equipment.

- **Adapting legacy systems:** According to officials at most of the five selected agencies, most manufacturers, and all integrators we spoke

[21] OMB-06-18.

to, integrating new physical access control systems' equipment with existing legacy systems can be challenging. Some stakeholders told us that integrating new physical access control systems with old equipment is often more difficult and more costly than starting from scratch.[22] As an illustration of this difficulty, TSA officials told us that integrating new physical access control system equipment with legacy systems has contributed to delays in the integration of TSA's newly installed physical access control system equipment. Partly as a result, only one TSA region is currently integrated into DHS' agency-wide network.

- **Security concerns about integrating physical access control systems:** Officials at two of the selected agencies and one system integrator we spoke to told us that some agency officials are reluctant to more fully integrate their physical access control systems. This reluctance is due to concern about a perceived increase in security risks resulting from more broadly networking physical access control systems' equipment and access credentials like PIV cards. However, other federal officials told us that this concern is unfounded. According to these officials, integrating agencies' physical access control systems will enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by electronically authenticating the validity of access credentials.
- **Lack of trained agency officials:** Stakeholders told us they believe that some federal agency officials have limited knowledge of physical access control system requirements. According to most physical access control systems' manufacturers and integrators we spoke to, federal agencies' contracting officers commonly lack sufficient understanding of federal physical access control system requirements. This insufficient understanding of physical access control system requirements may lead contracting officers to award contracts for the installation of physical access control systems to under-qualified integrators, which can lead to systems being improperly deployed or integrated. These experts said that this

[22] One DHS official commented that the Approved Products List provides the end-to-end configuration for a new physical access control system, but since most agencies have existing systems, they need to be retrofitted with the appropriate validation system and readers, and then specially configured through information technology support and approval processes in order to function in accordance with the Approved Products List. This creates a situation where agencies may not be able to completely follow the Approved Products List when adding on to an existing system that is still in transition to Approved Products List-compliance. In short, simply procuring an Approved Products List-system does not equal achieving FIPS-201 compliance.

situation could lead to security vulnerabilities at these agencies and expensive future costs. OMB staff told us that it may be desirable to raise agencies' awareness of federal physical access control system requirements, and a DHS official told us that this issue could be addressed by the training of program staff by GSA who support contracting officers.

OMB staff and officials from ISC and GSA indicated that they are aware of some of the challenges described above, as well as the possibility that some may be more broadly present across the federal government. Staff said that OMB and GSA are working with ISC to develop a consolidated guidance document concerning federal identification credentials. However, OMB staff told us that this guidance is primarily intended to consolidate and replace existing guidance documents, and does not contain new information related to the challenges identified by the selected agencies or other stakeholders we spoke to. Best practices that we have previously identified indicate that an interagency mechanism, such as an interagency group led by component or program-level staff, can help federal agencies address policy and program challenges. The guidance of such an interagency group could help agencies to address the challenges that we identified and that are related to implementing physical access control systems. [23]

ISC, with its unique role in addressing interagency security issues, is well-positioned to assess how the physical security community can help to address the government-wide challenges with physical access control system implementation. For example, ISC is well-positioned to determine through its membership the extent to which the challenges we identified are present across the federal government. In addition, ISC may be able to harness recent interagency efforts, such as the interagency information sharing and collaboration that produced ISC's guidance on planning and managing security resources, to develop guidance addressing agencies' cost issues through the mechanisms that we have previously identified, such as leveraging resources. Further, working with GSA, ISC could help to resolve confusion about which Schedule is the appropriate contracting vehicle, to the extent that this lack of clarity persists. ISC may also be positioned to provide a venue for information sharing to allow agencies to address training needs, such as those related to technical challenges, associated with legacy equipment and establish compatible policies to address this challenge. Finally, ISC's experience with interagency

[23] GAO-12-1022.

communication and collaboration could also facilitate agencies' response to concerns about the benefits of interoperable physical access control systems, and could work to reach consensus on the matter. According to a senior ISC official, the ISC has updated its countermeasures standard to assist the physical security community to better understand the references and policies associated with procuring and installing physical access control systems. Additionally, an ISC official told GAO that the ISC has approved commissioning a working group to assess what additional guidance related to physical access control would be beneficial for to the federal physical security community. However, without a government-wide review of the challenges we have identified, those challenges will be difficult to overcome. If these issues are not addressed, the fully interoperable, physical access control system network envisioned post September 11, 2001, and the increased security and efficiency that it would entail, will be difficult to attain.

Conclusions

OMB and GSA have taken various actions to help federal agencies implement GSA-approved physical access control systems. However, selected agencies have made limited progress, and have faced challenges that impede their progress. Lacking a baseline level of information on adherence to physical access control system requirements prevents OMB from gauging the level of progress being made by agencies. Likewise, an increased understanding of the extent and nature of the challenges that federal agencies may face as they implement physical access control systems may help enhance adherence to physical access control system requirements. This two-pronged approach, the establishment of a baseline and a better understanding of the challenges agencies face as they implement physical access control systems, could prove beneficial in achieving the vision of secure, interoperable systems across departments and agencies.

Recommendations for Executive Action

We are making one recommendation to OMB, and one recommendation to DHS.

- The Director of OMB should determine a government-wide baseline level of progress in meeting physical access control system requirements, including implementation of GSA-approved systems,

and should monitor progress in meeting these requirements. (Recommendation 1)

- The Secretary of Homeland Security should direct the ISC, in collaboration with member agencies, to assess the extent of, and develop strategies to address, government-wide challenges to implementing physical access control systems. (Recommendation 2)

Agency Comments

We provided a draft of this report to the Departments of Commerce, Justice, and Homeland Security, EPA, GSA, and OMB for their review and comment. DHS, GSA, and OMB provided technical comments, which we incorporated as appropriate. DHS provided written comments and concurred with our recommendation. DHS's comments are reprinted in appendix II. OMB staff told us that they did not have a comment on our recommendation. The Departments of Commerce and Justice and EPA did not have any comments on our report.

We will send copies of this report to the Ranking Member, Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives and the Secretaries of Commerce and Homeland Security, the Assistant Attorney General for the Department of Justice, the Administrator of the General Services Administration, the Director of the Office of Management and Budget, and the Acting Administrator of the Environmental Protection Agency. In addition, the report is 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 rectanusl@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 key contributions to this report are listed in appendix III.

Lori Rectanus
Director, Physical Infrastructure

Appendix I: Objectives, Scope, and Methodology

Our objectives were: (1) to assess the steps the Office of Management and Budget (OMB) and the General Services Administration (GSA) have taken to fulfill their government-wide responsibilities related to physical access control system implementation requirements and (2) to identify challenges selected federal agencies face in adhering to federal physical access control system requirements.

To assess the steps OMB and GSA have taken to fulfill their government-wide efforts to implement Homeland Security Presidential Directive 12's (HSPD-12) requirements, and to assess progress in these efforts, we interviewed OMB and GSA about their efforts to ensure that agencies meet the requirement to use GSA's Approved Products List. We also asked them to provide data, if available, on agencies' Approved Products List usage. We interviewed seven physical access control system manufacturers (AMAG, Gallagher Group, HID Global, Identiv, Lenel, Software House, and XTec), five integrators (contractors that install the equipment and connect it to agency networks with software) (Convergint Technologies, Chenega Corporation, MC Dean, Parsons, and Systems Engineering, Inc.), as well as other industry organizations—GSA Schedules Inc., the Secure Technology Alliance, and CertiPath— based on multiple recommendations from previous interviews.

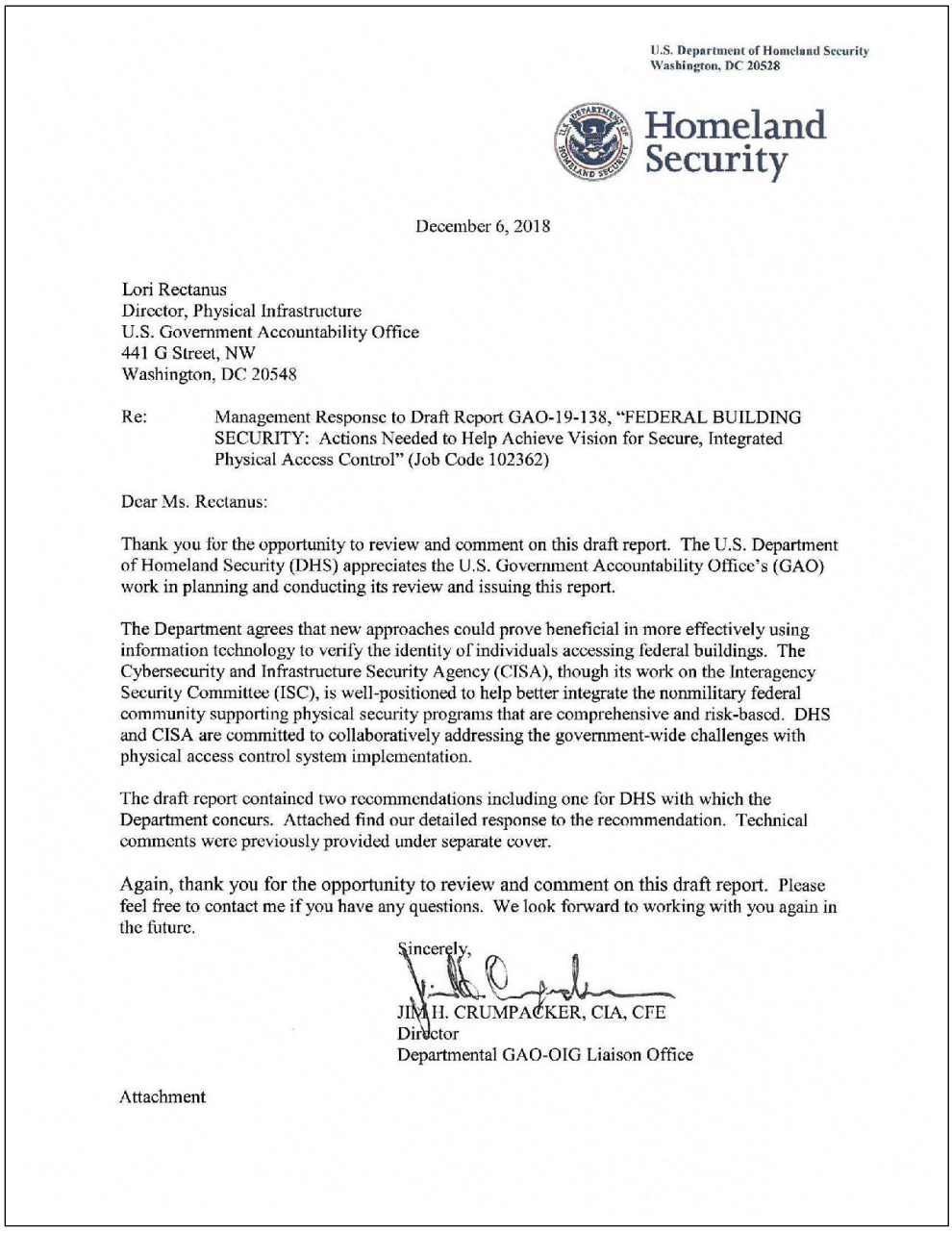
To identify illustrative examples of the progress that individual agencies have made in using the Approved Products List and implementing other HSPD-12 requirements, as well as the challenges that they have faced in doing so, we selected five executive branch agencies. These included (1) U.S. Coast Guard in the Department of Homeland Security (DHS); (2) Bureau of Prisons in the Department of Justice; (3) Transportation Security Agency in DHS; (4) Environmental Protection Agency (EPA); and (5) GSA. We interviewed officials from these agencies about the Approved Products List and collected data on agencies' purchases of GSA-approved physical access control system equipment using the Approved Products List since 2013. Our criteria for agency selection included agencies with facilities (1) held by non-defense executive branch agencies; (2) located in the United States; (3) totaling 200 or more buildings; and, (4) that are geographically dispersed (having buildings in

10 or more states). We also gave consideration to agencies with large numbers of buildings (choosing four larger, one smaller) and selected at least two agencies with homeland security responsibilities. We limited our scope to non-defense agencies because we have ongoing work related to these issues at the Department of Defense. We also requested and reviewed documents concerning Approved Products List usage and physical access control systems' deployment from each of these five selected agencies. Our use of the term stakeholders may include agencies, physical access control manufacturers, integrators, and knowledgeable organizations or officials. Results from our interviews with the selected agencies cannot be generalized. To identify the challenges most frequently cited by agencies, manufacturers, integrators, and other stakeholders, we conducted an analysis of our interviews, reviewed documents provided by agencies, and performed a literature review. In addition to considering the range of federal requirements related to physical access control, we considered relevant internal control standards from federal standards for internal-control in the areas of monitoring, enforcement, planning, and training and collaboration best practices identified in prior GAO work.[1] Further, we reviewed other relevant documents including GAO reports, GSA documentation, OMB memorandums, National Institute of Standards and Technology standards, Interagency Security Committee guidance, a report from the DHS Office of the Inspector General, and additional federal guidance related to physical access control systems.

We conducted this performance audit from October 2017 to December 2018 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.

[1] GAO-14-704G and GAO-12-1022.

Appendix II: Comments from the Department of Homeland Security



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

Homeland Security

December 6, 2018

Lori Rectanus
Director, Physical Infrastructure
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-138, "FEDERAL BUILDING SECURITY: Actions Needed to Help Achieve Vision for Secure, Integrated Physical Access Control" (Job Code 102362)

Dear Ms. Rectanus:

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) work in planning and conducting its review and issuing this report.

The Department agrees that new approaches could prove beneficial in more effectively using information technology to verify the identity of individuals accessing federal buildings. The Cybersecurity and Infrastructure Security Agency (CISA), though its work on the Interagency Security Committee (ISC), is well-positioned to help better integrate the nonmilitary federal community supporting physical security programs that are comprehensive and risk-based. DHS and CISA are committed to collaboratively addressing the government-wide challenges with physical access control system implementation.

The draft report contained two recommendations including one for DHS with which the Department concurs. Attached find our detailed response to the recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Attachment: Management Response to the Recommendation Contained in GAO 19-138

GAO recommended that the Secretary of Homeland Security:

Recommendation 2: Direct the ISC, in collaboration with member agencies, to assess the extent of, and develop strategies to address, government-wide challenges with physical access control system implementation.

Response: Concur. The ISC, which is chaired by the CISA Director of the Infrastructure Security Division, has already taken a number of actions responsive to this recommendation. These include:

1. on October 6, 2017, the ISC issued a memorandum to its members reminding them of the requirement to field Physical Access Control Systems from the "Approved Products List"; andproviding a comprehensive list of references to help them meet existing policies and technical requirements,
2. on October 1, 2018, the ISC codified these same requirements in the 2018 edition of "The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard" (See: "Appendix B: Countermeasures to the Risk Management Process for Federal Facilities"), an ISC standard to increase compliance with Homeland Security Presidential Directive 12 when procuring and installing Physical Access Control Systems, and
3. on November 15, 2018, the ISC's Steering Subcommittee approved the formation of a Physical Access Control Working Group to develop a document for the Federal security community identifying how to best meet the requirements laid out in existing policies and directives. Estimated Completion Date: November 30, 2019.

2

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contacts

Lori Rectanus, (202) 512-2834 or rectanusl@gao.gov

Staff Acknowledgments

In addition to the individual name above, Dave Sausville (Assistant Director); Kieran McCarthy (Analyst in Charge); Adam Gomez; Cam Flores; Elizabeth Wood; Josh Ormond; and Melissa Bodeau made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

Text of Appendix II: Comments from the Department of Homeland Security

Page 1

December 6, 2018

Lori Rectanus
Director, Physical Infrastructure
U.S. Government Accountability Office 441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-138, “FEDERAL BUILDING SECURITY: Actions Needed to Help Achieve Vision for Secure, Integrated Physical Access Control” (Job Code 102362)

Dear Ms. Rectanus:

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) work in planning and conducting its review and issuing this report.

The Department agrees that new approaches could prove beneficial in more effectively using information technology to verify the identity of individuals accessing federal buildings. The Cybersecurity and Infrastructure Security Agency (CISA), though its work on the Interagency Security Committee (ISC), is well-positioned to help better integrate the nonmilitary federal community supporting physical security programs that are comprehensive and risk-based. DHS and CISA are committed to collaboratively addressing the government-wide challenges with physical access control system implementation.

The draft report contained two recommendations including one for DHS with which the Department concurs. Attached find our detailed response

to the recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Page 2

Attachment: Management Response to the Recommendation Contained in GAO 19-138

GAO recommended that the Secretary of Homeland Security:

Recommendation 2:

Direct the ISC, in collaboration with member agencies, to assess the extent of, and develop strategies to address, government-wide challenges with physical access control system implementation.

Response:

Concur. The ISC, which is chaired by the CISA Director of the Infrastructure Security Division, has already taken a number of actions responsive to this recommendation. These include:

1. on October 6, 2017, the ISC issued a memorandum to its members reminding them of the requirement to field Physical Access Control Systems from the "Approved Products List"; and providing a comprehensive list of references to help them meet existing policies and technical requirements,

2. on October 1, 2018, the ISC codified these same requirements in the 2018 edition of "The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard" (See: "Appendix B:

Countermeasures to the Risk Management Process for Federal Facilities"), an ISC standard to increase compliance with Homeland Security Presidential Directive 12 when procuring and installing Physical Access Control Systems, and

3. on November 15, 2018, the ISC's Steering Subcommittee approved the formation of a Physical Access Control Working Group to develop a document for the Federal security community identifying how to best meet the requirements laid out in existing policies and directives. Estimated Completion Date: November 30, 2019.

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 website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548