



December 2014

FEDERAL FACILITY CYBERSECURITY

DHS and GSA Should Address Cyber Risk to Building and Access Control Systems

GAO Highlights

Highlights of [GAO-15-6](#), a report to congressional requesters

Why GAO Did This Study

Federal facilities contain building and access control systems—computers that monitor and control building operations such as elevators, electrical power, and heating, ventilation, and air conditioning—that are increasingly being connected to other information systems and the Internet. The increased connectivity heightens their vulnerability to cyber attacks, which could compromise security measures, hamper agencies' ability to carry out their missions, or cause physical harm to the facilities or their occupants.

GAO's objective was to examine the extent to which DHS and other stakeholders are prepared to address cyber risk to building and access control systems in federal facilities. GAO reviewed DHS's and other stakeholders' authorities to protect federal facilities from cyber attacks; visited selected FPS-protected facilities to determine what stakeholders were doing to address cyber risks to these systems; and interviewed experts about the cyber vulnerability of building and access control systems and related issues. GAO also reviewed GSA's security assessment process and a sample of reports.

What GAO Recommends

GAO recommends that DHS (1) develop and implement a strategy to address cyber risk to building and access control systems and (2) direct ISC to revise its *Design-Basis Threat* report to include cyber threats to building and access control systems. GAO also recommends that GSA assess cyber risk of its building control systems fully reflecting FISMA and its guidelines. DHS and GSA agreed with the recommendations.

View [GAO-15-6](#). For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

December 2014

FEDERAL FACILITY CYBERSECURITY

DHS and GSA Should Address Cyber Risk to Building and Access Control Systems

What GAO Found

The Department of Homeland Security (DHS) has taken preliminary steps to begin to understand the cyber risk to building and access controls systems in federal facilities. For example, in 2013, components of DHS's National Protection and Programs Directorate (NPPD) conducted a joint assessment of the physical security and cybersecurity of a federal facility. However, significant work remains.

- **Lack of a strategy:** DHS lacks a strategy that: (1) defines the problem, (2) identifies the roles and responsibilities, (3) analyzes the resources needed, and (4) identifies a methodology for assessing this cyber risk. A strategy is a starting point in addressing this risk. The absence of a strategy that clearly defines the roles and responsibilities of key components within DHS has contributed to a lack of action within the Department. For example, no one within DHS is assessing or addressing cyber risk to building and access control systems particularly at the nearly 9,000 federal facilities protected by the Federal Protective Service (FPS) as of October 2014. According to an NPPD official, DHS has not developed a strategy, in part, because cyber threats involving these systems are an emerging issue. By not developing a strategy document for assessing cyber risk to facility and security systems, DHS and, in particular, NPPD have not effectively articulated a vision for organizing and prioritizing efforts to address the cyber risk facing federal facilities that DHS is responsible for protecting.
- **Cyber threat not identified in report for federal agencies:** The Interagency Security Committee (ISC), which is housed within DHS and is responsible for developing physical security standards for nonmilitary federal facilities, has not incorporated cyber threats to building and access control systems in its *Design-Basis Threat* report that identifies numerous undesirable events. An ISC official said that recent active shooter and workplace violence incidents have caused ISC to focus its efforts on policies in those areas first. Incorporating the cyber threat to building and access control systems in the *Design-Basis Threat* report will inform agencies about this threat so they can begin to assess its risk. This action also could prevent federal agencies from expending limited resources on methodologies that may result in duplication.

GSA has not fully assessed the risk of building control systems to a cyber attack in a manner that is consistent with the Federal Information Security Management Act of 2002 (FISMA) or its implementation guidelines. Although GSA has assessed the security controls of these systems, the assessments do not fully assess the elements of risk (e.g., threat, vulnerability, and consequence). GSA also has not yet conducted security control assessments for many of its building control systems. GSA information technology officials said that GSA has conducted security assessments of the building control systems that are in about 500 of its 1,500 FPS-protected facilities and plans to complete the remainder in fiscal year 2015 or when systems are connected to the network or the Internet. Further, our review of 20 of 110 of the security assessment reports that GSA prepared during 2010 to 2014 showed that they were not comprehensive or fully consistent with FISMA implementation guidelines. For example, 5 of the 20 reports we reviewed showed that GSA assessed the building control device to determine if a user's identity and password were required for login but did not assess the system to determine if password complexity rules were enforced. This could potentially lead to weak or insecure passwords being used to secure building control systems.

Contents

Letter		1
	Background	4
	DHS and Other Stakeholders Are Taking Preliminary Steps to Address Cyber Risk to Building and Access Control Systems, but Significant Work Remains	15
	Conclusions	23
	Recommendations for Executive Action	24
	Agency Comments	24
Appendix I	Objective, Scope, and Methodology	26
Appendix II	Sources of Cyber-Based Threats and Types of Exploits	28
Appendix III	Comments from the Department of Homeland Security	30
Appendix IV	Comments from the General Services Administration	32
Appendix V	GAO Contact and Staff Acknowledgments	33
Related GAO Products		34
Tables		
	Table 1: Selected Federal Laws and Policies Governing the Protection of Building and Access Control Systems	8
	Table 2: Sources of Cyber-Based Threats	28
	Table 3: Types of Exploits	29
Figures		
	Figure 1: DHS's NPPD Offices with Facility Security or Cybersecurity Responsibilities	5

Figure 2: Some Types of Building and Access Control Systems in a Federal Facility	11
Figure 3: Example of the Connectivity of a Heating, Ventilation, and Air-Conditioning System via the Internet	13

Abbreviations

DHS	Department of Homeland Security
GSA	General Services Administration
FISMA	Federal Information Security Management Act of 2002
FPS	Federal Protective Service
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISC	Interagency Security Committee
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
<i>PPD-21</i>	<i>Presidential Policy Directive 21</i>
<i>RMP</i>	<i>The Risk Management Process for Federal Facilities</i>
US-CERT	U.S. Computer Emergency Readiness Team

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



December 12, 2014

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Patrick Meehan
Chairman
Subcommittee on Cybersecurity, Infrastructure Protection, and Security
Technologies
Committee on Homeland Security
House of Representatives

The Honorable Jeff Duncan
Chairman
Subcommittee on Oversight and Management Efficiency
Committee on Homeland Security
House of Representatives

The Department of Homeland Security (DHS) is responsible for protecting federal facilities, including thousands of office buildings, laboratories, and warehouses, which are part of the nation’s critical infrastructure. These facilities contain building and access control systems such as heating, ventilation, and air conditioning; electronic card readers; and closed-circuit camera systems that are increasingly being automated and connected to other information systems or networks and the Internet.¹ As these systems are becoming more connected, their vulnerability to potential cyber attacks² is also increasing. This was demonstrated by an incident in 2009, when a security guard at a Dallas-area hospital loaded a

¹According to the National Institute on Standards and Technology, an “information system” is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems can include diverse entities ranging from high-end supercomputers, workstations, personal computers, cellular telephones, and personalized digital assistants to very specialized systems such as weapons systems, telecommunications systems, industrial/process control systems, and environmental control systems.

²“Cyber attacks” are defined as attacks conducted via cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling computer infrastructure, destroying the integrity of the data, or stealing controlled information.

malicious program onto the hospital's computers, one of which controlled the heating, ventilation, and air-conditioning control system for two floors, which, according to court records, could have affected patients' medications and treatments. Security officials we interviewed also said that cyber attacks on systems in federal facilities could compromise security countermeasures, hamper agencies' ability to carry out their missions, or cause physical harm to the facilities and their occupants.

Although DHS's Federal Protective Service (FPS) is responsible for the physical security of facilities under the custody and control of the General Services Administration (GSA), other entities may own and operate these building and access control systems. For example, GSA or private building owners may own and operate heating, ventilation, and air-conditioning systems, and federal tenant agencies may own access control systems and have responsibility for protecting them. However, the extent to which DHS and other stakeholders are prepared to assess and mitigate cyber risk—a measure of the extent to which an entity is threatened by a potential circumstance or event—to these systems is unclear. We have identified the protection of federal information systems as a government-wide high-risk area since 1997 and in 2003 expanded this high-risk area to include the protection of systems supporting our nation's critical infrastructure, a designation that remains in place today.³ Moreover, concern about protecting federal facilities is one of the main reasons why we have designated federal real property management as a high risk area.⁴

This report focuses on building and access control systems used to operate or protect these facilities, and does not address cyber risk to other types of information systems or networks. You asked us to review FPS's efforts to protect federal facilities from these types of cyber attacks. This report examines the extent to which DHS and other stakeholders are prepared to address cyber risk to building and access control systems in FPS-protected facilities.

To conduct our evaluation, we analyzed relevant homeland security and cybersecurity-related laws, policies, and guidance. We identified relevant federal stakeholders, for example, DHS and its various components,

³GAO, *High Risk Series: An Update*, [GAO-13-283](#) (Washington, D.C.: February, 2013).

⁴[GAO-13-283](#).

including the National Protection and Programs Directorate (NPPD), FPS, the Office of Infrastructure Protection, the Office of Cyber and Infrastructure Analysis, and the Office of Cybersecurity and Communications and its subcomponents: Federal Network Resilience and the National Cybersecurity and Communications Integration Center (NCCIC) and its subcomponents, the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). We also identified the Interagency Security Committee, GSA, and other federal agencies that are tenants in facilities protected by FPS. We interviewed each of these stakeholders or their relevant components to determine what steps they have taken to prevent cyber attacks on building and access control systems in FPS-protected facilities. We identified and visited five FPS-protected facilities in the Washington, D.C., area to determine what FPS and other stakeholders are doing to assess and mitigate cyber risk to building and access control systems in these facilities. We selected these facilities to represent different types of ownership (three were government-owned and two were leased from private owners), different security levels,⁵ and uses. We chose to visit facilities in the Washington, D.C., area because of the large number of federal facilities that met these criteria. At each of the five facilities, we interviewed officials from FPS, GSA (or the facility's owner if leased), and tenant agencies about their roles and responsibilities for securing these systems. The findings from these site visits are not generalizable to all FPS-protected facilities. We also reviewed GSA's security assessment procedures and a sample of GSA's security assessment reports on building systems that were prepared between 2010 and 2014, and discussed them with agency information technology officials. The findings from those reviews are not generalizable to all of GSA's assessment reports.

In addition, we conducted a literature review and interviewed DHS officials and experts about the extent to which building and access control systems are vulnerable to cyber attacks and the possible consequences of such attacks. Ten experts with cybersecurity expertise were selected from academia and private industry. These experts were chosen through our research and based on interviews during previous cybersecurity reviews. Their views are not generalizable. A list of related GAO products

⁵Facility security levels are assigned to all federal, nonmilitary facilities based on criteria such as mission criticality, symbolism, and facility size and population. Levels range from one (lowest) to five (highest).

on cybersecurity is provided at the end of this report. Appendix I provides more details about our scope and methodology.

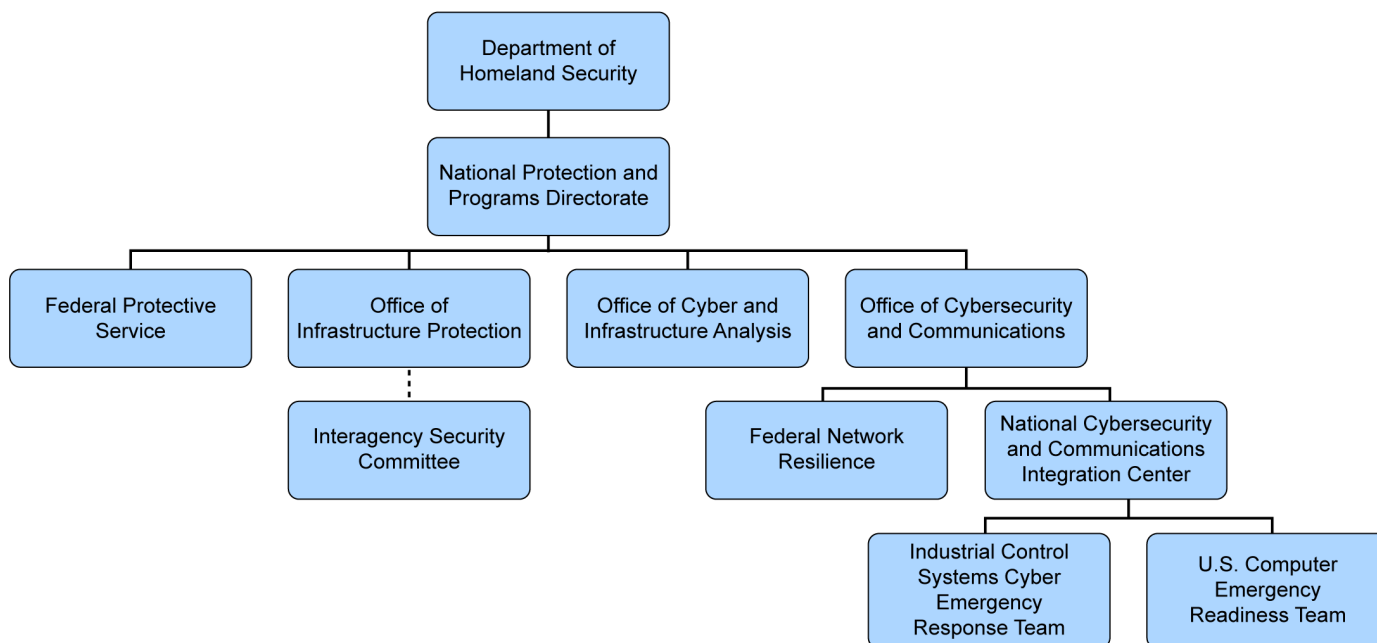
We conducted this performance audit from November 2013 through December 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

DHS and Other Stakeholders Are Involved in Physical and Cybersecurity of Federal Facilities

The Homeland Security Act of 2002 requires DHS, among other things, to protect federal facilities as well as people on the property. Within DHS, the National Protection and Programs Directorate (NPPD) is responsible for leading the national effort to strengthen the security and resilience of the nation's physical and cyber-critical infrastructure against terrorist attacks, cyber events, natural disasters, or other catastrophic incidents. As part of this effort, an NPPD responsibility is to lead the effort to strengthen security and resilience of federal facilities and federal (nonmilitary) information systems and networks. Figure 1 shows several NPPD components responsible for issues related to protecting federal facilities or cybersecurity.

Figure 1: DHS's NPPD Offices with Facility Security or Cybersecurity Responsibilities



Source: GAO analysis of DHS information. | GAO-15-6

- FPS is responsible for protecting nearly 9,000 federal facilities⁶ from physical attacks. As part of its facility protection mission, FPS conducts facility security assessments and recommends countermeasures, and provides law enforcement services to its protected facilities.⁷
- The Office of Infrastructure Protection is responsible for leading efforts to strengthen critical infrastructure security and resilience against all hazards, which include both physical and cyber attacks.
- The Office of Cyber and Infrastructure Analysis is responsible for, among other things, providing analytic support to DHS leadership, assessing and informing national critical infrastructure risk-management strategies, and developing or enhancing capabilities to support crisis action by identifying and prioritizing infrastructure.

⁶As of October 2014.

⁷To fund its operations and contract guard program, federal tenant agencies in GSA-controlled facilities provide funding to FPS.

-
- The Office of Cybersecurity and Communications is responsible for enhancing the security, resilience, and reliability of the nation’s cyber and communications infrastructure.
 - Within the Office of Cybersecurity and Communications, Federal Network Resilience is to identify common cybersecurity requirements across the federal government, collaborate with agencies to identify solutions, implement policy and technical solutions, and monitor the effectiveness of implemented solutions.
 - Within the Office of Cybersecurity and Communications, the National Cybersecurity and Communications Integration Center (NCCIC) is responsible for operating an around-the-clock cyber situational awareness; incident response; and the management center for the federal government, intelligence community, and law enforcement. Two NCCIC subcomponents—the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)—are responsible for carrying out the NCCIC’s cyber incident reporting and response functions.
 - US-CERT is responsible for providing analysis and information about malicious activity threatening the nation’s networks, and provides a cyber reporting and response function to federal information system operators. For federal entities, reporting federal information security incidents to US-CERT is mandatory under reporting guidance established in accordance with the Federal Information Security Management Act of 2002 (FISMA).⁸
 - ICS-CERT provides similar reporting and response functions for operators of control systems inside and outside of the federal government. Control systems are computers that are used to monitor and control sensitive processes and physical functions. Building systems generally employ control systems in their operations.

⁸Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (codified, as amended, at 44 U.S.C. § 3541-3549).

-
- The Interagency Security Committee (ISC), a DHS-chaired organization comprised of 54 member agencies that is housed within the Office of Infrastructure Protection, is responsible for establishing policies for security in and protection of buildings and facilities in the United States occupied by federal employees for nonmilitary activities.

GSA manages real property for many civilian federal agencies and has a large portfolio of owned and leased properties that it rents to its federal agency customers. GSA officials indicated that in federally-owned facilities, GSA is generally responsible for the building systems they contain. In privately-owned facilities, the private owner is generally responsible for the building systems. GSA officials also said that federal agencies that are tenants in facilities that are under the control and custody of GSA could also be responsible for certain systems if the tenant has custodial control of the system, such as an access control system for their space within a facility.

Selected Laws and Policies Relating to Physical and Cybersecurity of Federal Facilities

Table 1 shows some of the laws and policies that apply to federal facility physical security and cybersecurity.

Table 1: Selected Federal Laws and Policies Governing the Protection of Building and Access Control Systems

The Homeland Security Act of 2002	<p>Under section 1706 of the Homeland Security Act of 2002, DHS is required to</p> <ul style="list-style-type: none"> • protect the buildings, grounds, and property that are owned, occupied or secured by the federal government as well as the persons on the property, and • in performance of such duties DHS officers and agents are authorized to, among other things: <ul style="list-style-type: none"> • enforce federal laws and regulations for the protection of persons and property; and • investigate offenses against these properties and persons.⁹
The Federal Information Security Management Act of 2002	<p>FISMA requires, among other things, that</p> <ul style="list-style-type: none"> • each agency develop, document, and implement an information security program to include periodic assessments of risk, policies and procedures that are based on these risk assessments, security awareness training for its personnel, and periodic testing and evaluation of information security policies; • each agency prepare and maintain inventories of major information systems under their control and to develop procedures for detecting, reporting, and responding to security incidents; • the Department of Commerce’s National Institute of Standards and Technology (NIST) develop minimum information-security standards and guidelines for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems;¹⁰ • the Office of Management and Budget ensure the operation of a central federal information-security incident center that compiles and analyzes information about incidents that threaten information security and informs operators of agency information systems about current and potential threats and vulnerabilities; and • senior agency officials provide information security for the information and information systems that support the operations and assets under their control.

⁹Section 1315(a) of title 40, United States Code, provides in pertinent part that: “To the extent provided for by transfers made pursuant to the Homeland Security Act of 2002, the Secretary of Homeland Security...shall protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed-ownership corporation thereof) and the persons on the property.”

¹⁰Under FISMA, national security systems are defined to mean, among other things, those that involve intelligence activities, cryptologic activities related to national security, and command and control of military forces. See 44 U.S.C. § 3542(b)(2)(A).

NIST Standards and Guidelines	In accordance with FISMA, NIST is responsible for providing information security standards and guidelines for non-national security information and information systems. These guidelines implement FISMA requirements. Among other guidelines, NIST has published guidance for securing industrial control systems. ¹¹
Presidential Policy Directive 21	<p><i>Presidential Policy Directive 21 (PPD-21)</i>, issued in February 2013,¹² establishes the protection of critical infrastructure against both physical and cyber threats as national policy. More specifically, the directive</p> <ul style="list-style-type: none"> • requires DHS to provide strategic guidance to promote the security and resilience of the nation’s critical infrastructure; • tasks agency and department heads with the identification, prioritization, assessment, remediation, and security of their internal critical infrastructure that supports primary mission essential functions; • tasks GSA, in consultation with DHS and the Department of Defense, to provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights; • identifies sector lead agencies for 16 critical infrastructure sectors, including DHS and GSA as co-leads for the government facilities sector; and • identifies roles and responsibilities of sector lead agencies, which include serving as the day-to-day interface for the protection of critical infrastructure, to carry out incident management within the sector and provide support or technical assistance in assessing vulnerabilities in the sector.

Source: GAO analysis. | GAO-15-6

Federal Facilities Contain Various Types of Building and Access Control Systems

As shown in figure 2, some types of building and access control systems in federal facilities include:

- **closed circuit camera systems** include cameras, televisions or monitors, and recording equipment, and provide video surveillance capabilities;
- **access control systems** include card readers, control panels, access control servers, and infrastructure such as door actuators and communications lines, which restrict access to authorized persons only;
- **fire annunciation and suppression systems** include fire alarms, emergency communication equipment, and water-based or non-water-based suppression systems, designed to prevent, extinguish, or control a fire or other life safety event;

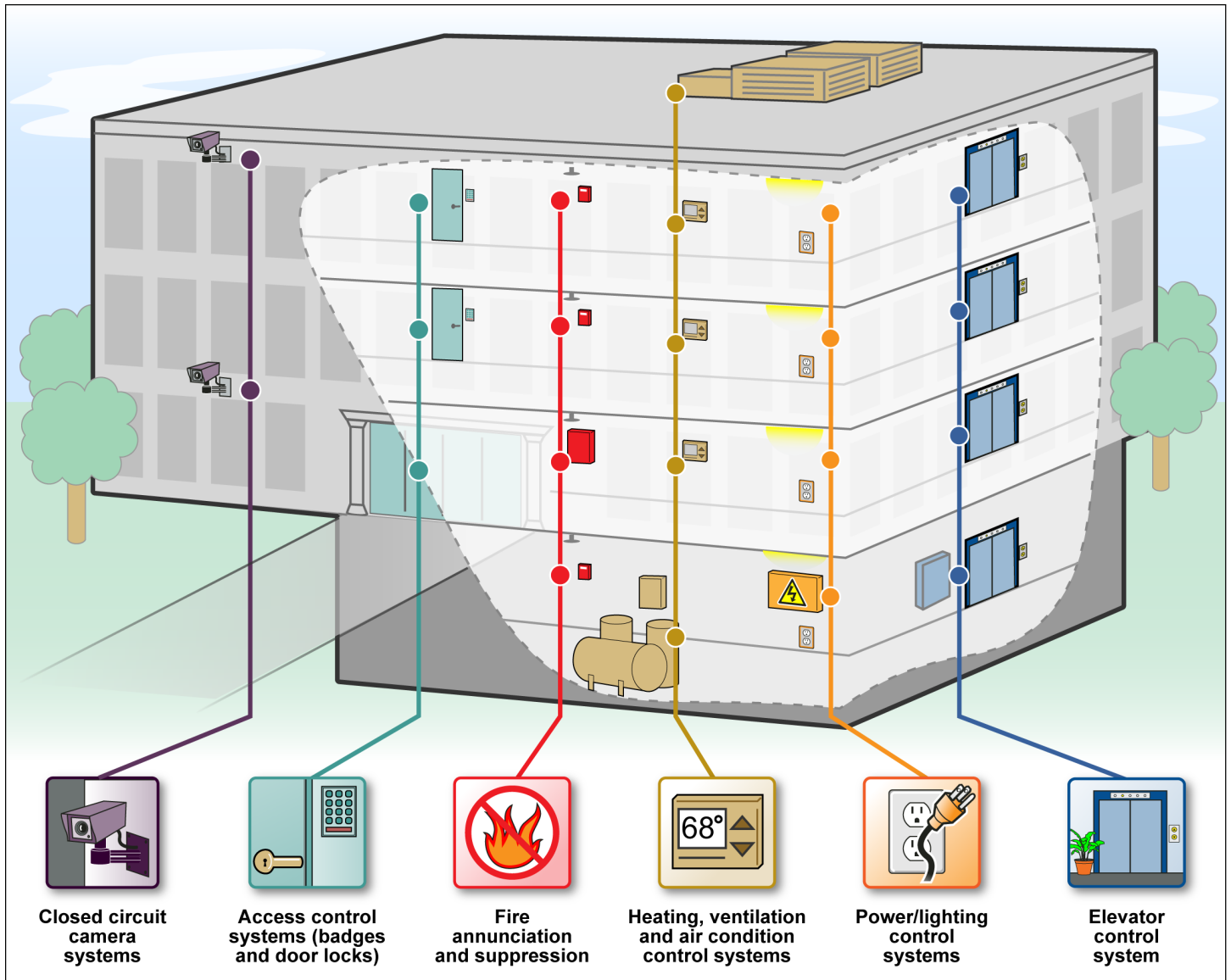
¹¹National Institute of Standards and Technology, *Special Publication 800-82 (Revision 1), Guide to Industrial Control Systems (ICS) Security* (Gaithersburg, Md.: May 2013). Industrial control systems are used to monitor and control highly sensitive processes throughout the energy, transportation, manufacturing, and other sectors. NIST officials said that industrial control systems across sectors, including federal facilities, share similar characteristics and that many of the recommendations from the guide are applicable and could be used as a reference for protecting such systems against cybersecurity threats.

¹²*Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

-
- **heating, ventilation, and air conditioning systems** include equipment for heating, cooling, moisture control, ventilation or air handling, and measurement and control, often managed through a building automation system¹³;
 - **power and lighting control systems** include lighting devices and their controls, advanced-metering controls, power distribution systems, and emergency power or lighting systems, which are also often managed through a building automation system; and
 - **elevator control systems** include operating machinery, safety systems, and a control system or panel.

¹³Building automation systems, also known as energy management control systems, provide centralized control—through the use of software and hardware (e.g., computer, modems, sensors, controllers, and printers)—to monitor and adjust building systems (e.g., temperature settings and schedules for running equipment)—such as a building’s cooling systems. A building automation system is intended to optimize the integrated performance of the individual equipment’s components that comprise the system. Data can be recorded so they can be analyzed.

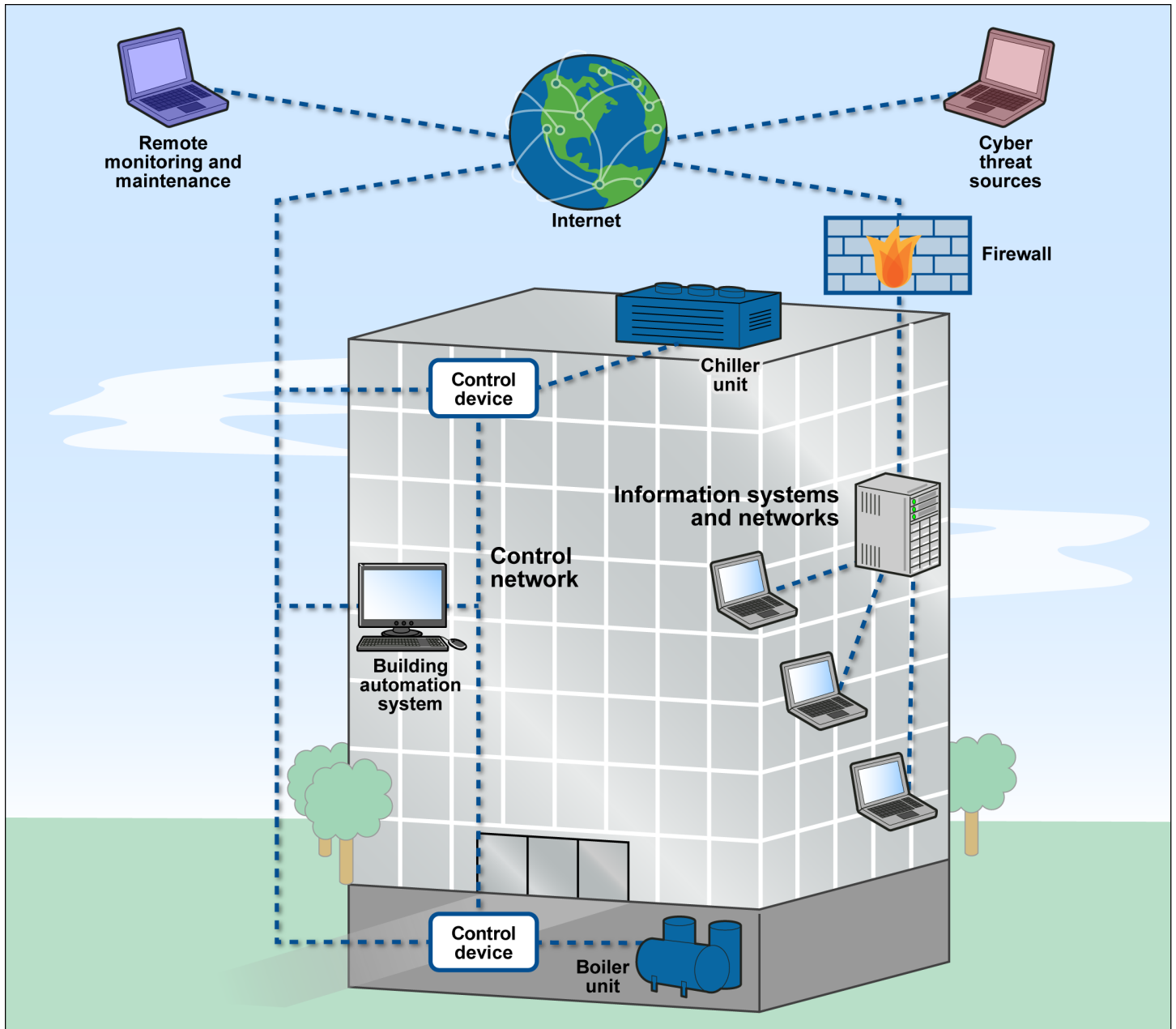
Figure 2: Some Types of Building and Access Control Systems in a Federal Facility



Source: GAO. | GAO-15-6

To increase efficiency, centralized control of building and access control systems is increasingly achieved through automation systems. Building and access control systems, automation systems, and the devices within them, are now often configured with connections to the Internet. These Internet connections allow the systems to be accessed remotely, for example, to receive software patches and updates. Figure 3 shows an example of a facility where a heating, ventilation, and air-conditioning system is managed through a building automation system and operated over a control network. In this example, the information systems and networks used by this building's tenant are protected by a firewall—a common cybersecurity countermeasure—while the control network and its devices have direct Internet connectivity.

Figure 3: Example of the Connectivity of a Heating, Ventilation, and Air-Conditioning System via the Internet



Source: GAO. | GAO-15-6

Sources of Cyber Threats to Building and Access Control Systems

Cyber threats are any circumstance or event with the potential to adversely affect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service. Cyber threat sources include corrupt employees, criminal groups, hackers, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary or political gain or mischief, among other things. Cyber threat sources may make use of various cyber techniques, or exploits, to adversely affect systems or networks. More detailed information on sources of cyber threats and types of exploits can be found in appendix II.

Insider threats—which can include disgruntled employees, contractors, or other persons abusing their positions of trust—also represent a significant threat to building and access control systems, given their access to and knowledge of these systems. This threat results in standalone systems (those with no external network connections) also being at risk.

Moreover, from fiscal year 2011 to fiscal year 2014, the number of cyber incidents reported to DHS involving industrial control systems, which include building and access control systems, increased from 140 incidents to 243 incidents, an increase of 74 percent. The following examples illustrate that these systems are at risk:

- In 2014, a federal agency reported a cyber incident at a wastewater treatment plant.¹⁴
- In 2013, the retailer Target experienced a breach in its payment card data, which the company believes occurred after intruders obtained a heating, ventilation, and air-conditioning system vendor's credentials to access the outermost portion of its network.
- In 2010, a sophisticated computer attack known as Stuxnet was discovered that targeted control systems used to operate industrial processes in the energy, nuclear, and other critical sectors.

¹⁴Details regarding this incident are law-enforcement sensitive and cannot be publicly disclosed.

-
- In 2009, a security guard at a Dallas-area hospital loaded a malicious program onto the hospital's computers, one of which controlled the heating, ventilation, and air-conditioning control system for two floors, which, according to court records, could have affected patients' medications and treatments.
 - In 2006, Los Angeles city employees hacked into computers controlling the city's traffic lights, an action that disrupted signal lights and caused substantial backups and delays.

Cybersecurity experts that we interviewed also generally said that building and access control systems are vulnerable to cyber attacks. One expert, for example, noted that control systems were not designed with cybersecurity in mind.

DHS and Other Stakeholders Are Taking Preliminary Steps to Address Cyber Risk to Building and Access Control Systems, but Significant Work Remains

DHS Does Not Have a Strategy to Address Cyber Risk to Building and Access Control Systems

DHS has taken preliminary steps to begin to understand the cyber risk to building and access controls systems but has not developed a strategy. Section 1706 of the Homeland Security Act of 2002 authorizes DHS to protect federal facilities and *PPD-21* requires it to provide strategic guidance to promote the security and resilience of the nation's critical infrastructure, which includes federal facilities, to cyber and physical threats. In addition, as we reported in 2013, implementing a comprehensive strategic approach to cybersecurity requires the development of a strategy to guide the activities that will support this

approach.¹⁵ In guidance that we developed to assist agencies implement the Government Performance and Results Act of 1993,¹⁶ we stated that developing a strategic plan can help clarify organizational priorities and unify employees in the pursuit of shared goals.

DHS, in particular NPPD, has taken preliminary steps to begin understanding the cyber risk to building and access control systems. For example, in 2013, NPPD components—including FPS, the Office of Infrastructure Protection, and ICS-CERT—conducted a joint assessment of the physical security and cybersecurity in a recently renovated GSA facility in the Washington, D.C., area.¹⁷ Also in 2013, FPS prepared a discussion paper for ISC identifying the types of building systems that could be assessed for cyber risk, including heating, ventilation, and air conditioning; access controls; closed-circuit video; fire annunciation panels; and security command and control centers. According to FPS’s discussion paper, to identify cyber vulnerabilities, assessments should be used to determine if these systems are connected and remotely operated and what security controls are in place, such as firewalls.

However, DHS has not developed a strategy that:

- defines the problem,
- identifies the roles and responsibilities,
- analyzes the resources needed, and
- identifies a methodology for assessing cyber risk to building and access control systems.

¹⁵GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, [GAO-13-187](#) (Washington, D.C.: Feb. 14, 2013).

¹⁶Pub.L.No. 103-62, 107 Stat. 285 (1993), See also Government Performance and Results Act Modernization Act of 2010, Pub. L. No. 111-352, 124 Stat. 3866 (2011).

¹⁷Each component used its own facility assessment tool or methodology. FPS used its Modified Infrastructure Survey Tool (MIST), the Office of Infrastructure Protection used the Infrastructure Survey Tool, and ICS-CERT performed an Architecture/Design Review Cyber Security assessment and a Network Architecture Verification and Validation analysis.

As we reported in 2013,¹⁸ a strategy is a starting point that defines the problem and risk intended to be addressed by organizations as well as plans for (1) tackling the problem and risk, (2) allocating and managing the appropriate resources, and (3) identifying different organizations' roles and responsibilities. In particular, the absence of a strategy that clearly defines the roles and responsibilities of key components within DHS has contributed to the lack of action within the Department. For example, no one within DHS is assessing or addressing cyber risk to building and access control systems particularly at the nearly 9,000 federal facilities protected by FPS.

In addition, because DHS has not developed a strategy, several components within DHS have made different assertions about their roles and responsibilities. For example, FPS's Deputy Director for Policy and Programs said that FPS's authority includes cybersecurity. However, FPS is not assessing cyber risk because, according to this official, it does not have the expertise. Furthermore, although ICS-CERT has developed a tool to assess cyber risk, it also is not assessing cyber risk to building and access control systems at federal facilities. Moreover, NPPD's Federal Network Resilience is to, among other things, identify common cybersecurity requirements across the federal government, but it also is not working on issues regarding the cyber risk of building and access control systems in the federal government. An official from the Office of the Under Secretary of NPPD acknowledged that NPPD has not yet determined roles and responsibilities, including what entity should conduct cyber risk assessments of FPS-protected facilities or what assessment tool should be used. This official said that the Department has not developed a strategy, in part, because cyber threats involving building and access control systems are an emerging issue.

The lack of a strategy was also reflected in DHS's guidance to federal agencies on reporting computer security incidents. Before October 1, 2014, DHS's guidance for federal agencies on reporting computer security incidents did not specify that information systems included industrial control systems. A DHS director said that the lack of clear guidance on reporting cyber incidents involving industrial control systems may have contributed to the lack of incident reporting by federal agencies. From fiscal year 2010 to August 2014, out of 851 reported industrial

¹⁸[GAO-13-187](#).

control system incidents, DHS received only one from a federal agency, which did not involve a building or access control system.¹⁹ On October 1, 2014, DHS issued guidance clarifying that information systems include industrial control systems and that federal agencies should report all information security incidents to US-CERT. A DHS official said that the guidance was clarified in part because of questions that we raised during our review.

By not developing a strategy for addressing cyber risk to building and access control systems, DHS and, in particular, NPPD, have not effectively articulated a vision for organizing and prioritizing efforts to address the cyber risk facing federal facilities that DHS is responsible for protecting. DHS also faces limitations in ensuring that its resources are allocated appropriately and not resulting in duplication. Furthermore, by not assessing the risk to these systems and taking steps to reduce that risk, federal facilities may be vulnerable to cyber attacks. Security officials at DHS and tenant agencies at FPS-protected facilities that we visited, as well as experts whom we interviewed, suggested various possible consequences of cyber attacks on these systems, including:

- allowing people to gain unauthorized access to facilities;
- damaging temperature-sensitive equipment, such as in data centers;
- causing life-safety systems such as fire alarms or sprinklers to give false alarms or fail to alarm in the event of an emergency, malfunctions that could result in injury or a loss of life;
- disabling facilities due to lack of power or other environmental needs;
- providing access to information systems;
- having to temporarily evacuate facilities; and
- damaging the government's credibility if it was unable to protect its employees.

¹⁹Details regarding this incident are law-enforcement sensitive and cannot be publicly disclosed.

ISC Has Not Incorporated Cybersecurity in Its Design-Basis Threat Report

Housed within DHS, ISC, which was established to enhance the quality and effectiveness of physical security in federal facilities, is responsible for developing physical security standards for nonmilitary federal facilities. However, it has not incorporated cybersecurity in its *Design-Basis Threat* report, which establishes the characteristics of the threat environment to be used in conjunction with all ISC standards.²⁰ The report, which identifies and describes numerous undesirable events under various scenarios and their probability of occurring as well as establishing a profile of the types, composition, and capabilities of adversaries, is applicable to all buildings and facilities in the United States occupied by federal employees for nonmilitary activities. Aside from certain intelligence-related exceptions, Executive Order 12977 requires executive branch departments and agencies to cooperate and comply with ISC's policies and recommendations, including any standards that ISC sets. Its standards are developed based on leading security practices across the government and set forth a decision-making process to help ensure that agencies have effective physical security programs in place.

According to ISC, the unpredictable nature of adversaries makes it difficult to determine what specific factors will make a facility an attractive target. However, ISC stated that because federal facilities include some highly symbolic federal and commercial office buildings, laboratories, and warehouses—some of which are used to store high-risk items such as weapons and drugs—this causes them to be more likely targets for adversaries or terrorists who attempt to disable a building or access control system in order to carry out an attack. Moreover, as we have previously reported, threats to systems supporting critical infrastructure and federal information systems are evolving and growing.²¹ The Director of National Intelligence has warned of the increasing globalization of cyber attacks, including those carried out by foreign militaries or organized international crime. In January 2012, he testified before Congress that such threats pose a critical national and economic security concern. To further highlight the importance of the threat, on October 11, 2012, the Secretary of Defense stated that the collective result of attacks

²⁰The *Design-Basis Threat* report is an appendix to ISC's physical security standard, *The Risk Management Process for Federal Facilities (RMP)*, with which federal executive branch agencies must comply. Among other things, the RMP includes standards for agencies' facility risk assessment methodologies.

²¹[GAO-13-187](#).

on our nation's critical infrastructure could be "a cyber Pearl Harbor, an attack that would cause physical destruction and the loss of life." An ISC official said that while ISC is concerned about cyber threats to federal facilities and is currently pursuing efforts to minimize them, it views this threat as one among a number of threats facing federal facilities. The official said that recent active shooter and workplace violence incidents have caused the membership to focus the committee's efforts on policies in those areas first. However, incorporating the cyber threat to building and access control systems in ISC's *Design-Basis Threat* report will inform agencies about this threat so they can begin to assess its risk. It also could prevent federal agencies from expending limited resources on methodologies that may result in duplication.

Use of ISC standards is beneficial because they are intended to 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. Although it is important to tailor physical security to facilities so that the unique risks at individual 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.

At three of the five FPS-protected facilities that we visited, we found that information technology officials varied in how they were securing the access control systems owned by their agencies. At one agency, the chief information security officer said that as part of securing an access control system that was connected to the agency's information network, his office conducts procedures to certify the security controls of the agency's information systems and to formally authorize and accept the risk associated with their operation. The official said the system is connected to the agency's information network to comply with *Homeland Security Presidential Directive 12*, which requires the establishment of a mandatory, government-wide standard for secure and reliable forms of identification for federal government employees and contractors. At another agency, officials said that its access control system was not connected to the agency's information network, but complied with FISMA requirements. Officials at a third facility said that its access control systems, which are not connected to the agency's information network, are part of its FISMA inventory. In addition, security officials at one of the facilities we visited said that they were not concerned with the cybersecurity of the security system that the agency owns because it is a standalone system. The officials said that they plan to upgrade the

security system in the near future, an upgrade that they said would comply with information security standards and policies, would be installed on the agency's network, and not have remote capability from outside the network.

An ISC official said that ISC is currently pursuing efforts to mitigate cyber threats. In 2013, ISC's Subcommittee on Convergence prepared a draft white paper, *Securing Government Assets through Combined Traditional Security and Information Technology*, on how security systems could be better protected through coordination between information technology and security officials. The draft white paper recommends that agency information and security officials develop memorandums of agreement and interagency service agreements defining roles and responsibilities for securing electronic security systems. The subcommittee chairman said that those recommendations directly apply to security systems such as access controls, cameras, and alarms and "loosely apply" to the other building systems. In September 2014, an ISC official said the Committee was incorporating comments from member agencies for final processing and that the white paper will be a report to help agencies achieve convergence between their physical security and information technology communities, and will not be a set of standards or guidance.

GSA Has Not Fully Assessed Cyber Risk to Its Building Control Systems in Federal Facilities

FISMA requires federal agencies to periodically assess the cyber risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets under their control. FISMA also requires the periodic testing and evaluation of the effectiveness of agency information security policies, procedures, and practices, including testing of management, operational, and technical controls of all major systems. To assist federal agencies with implementing FISMA requirements, NIST has issued standards and guidelines that are applicable to all non-national security information systems.²² One of those guides, NIST's *Risk Management Framework*,

²²NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39 (Gaithersburg, Md.: March 2011); *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Revision 1 (Gaithersburg, Md.: February 2010); and *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1 (Gaithersburg, Md.: September 2012).

states that organizations should assess security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

Neither GSA nor DHS (as mentioned earlier) is fully assessing the risk of building control systems that are in about 1,500 FPS-protected facilities²³ to a cyber attack. Instead, GSA has conducted security control assessments of these systems. However, these assessments are designed to determine the effectiveness of controls associated with a building control system and do not fully assess all elements of risk (e.g. the threat, vulnerability, and consequence) of the control system to a cyber attack.

Moreover, GSA has not conducted security control assessments for all of its systems that are in about 1,500 FPS-protected facilities. In November 2014, GSA information technology officials said that from 2009 to 2014, the agency conducted 110 security assessments of the building control systems that are in about 500 of its 1,500 facilities. GSA has not yet assessed the security of control systems with network or Internet connections in about 200 buildings. GSA officials stated that they plan to assess these systems during fiscal year 2015. According to these officials, GSA also plans to assess the security of standalone control systems in about 800 buildings when they are converted to network- and Internet-connected systems.

Further, our review of 20 of 110 of GSA's security assessment reports (between 2010 and 2014) show that they were not comprehensive and not fully consistent with NIST guidelines. For example, in 5 of the 20 reports we reviewed, GSA assessed the building control device to determine if a user's identity and password were required for login but did not assess the device to determine if password complexity rules were enforced. This could potentially lead to weak or insecure passwords being used to secure building control devices.

GSA also conducted its assessments of building control systems in a laboratory setting which allowed it to test components and to identify

²³These 1,500 facilities are ones that the federal government owns. GSA does not own the building system in leased facilities, which are the majority of facilities in its portfolio.

weaknesses in their default configuration. However, GSA does not conduct further assessments after installation when configuration settings may no longer reflect their default values. As a result, GSA has limited assurance that the configurations assessed reflect the configurations implemented in the facility, thereby increasing the risk that vulnerabilities in building control systems may not be detected.

In November 2014, GSA's Chief Information Officer said that GSA is conducting its security assessments in this manner because the agency's approach to assessing cyber risk to these systems is evolving. Until GSA fully and effectively assesses the information security over all of its building control systems, it will have diminished assurance that the systems' security controls are effectively implemented and operating as intended.

Conclusions

Because federal facilities are a part of the nation's critical infrastructure and include some highly symbolic federal and commercial office buildings, laboratories, and warehouses—some of which are used to store high risk items such as weapons and drugs—determining the extent to which building and access control systems within them are vulnerable to cyber attacks is critical to providing security. However, DHS faces challenges in determining the extent to which building and access control systems in federal facilities are vulnerable to cyber attacks because it lacks a strategy that defines the problem, identifies the roles and responsibilities for securing these systems, analyzes the resources needed to assess cyber risk to the systems, and a methodology for assessing cyber risk to building and access control systems. Moreover, without a strategy that addresses cyber risk to building and access control systems in federal facilities, key stakeholders, particularly within NPPD, do not have a clear understanding of their roles and responsibilities. And as a result, no one in DHS is assessing the cyber risk to building and access control systems at the almost 9,000 facilities protected by FPS. A strategy will help DHS to begin addressing this threat.

Federal agencies that own building and access control systems may be hampered in addressing cyber risk of building and access control systems because ISC has not identified this threat in its *Design-Basis Threat* report to federal agencies. According to experts and security officials we interviewed, not addressing this threat could result in disruptions of agency operations or harm to occupants of federal facilities. In addition, because GSA owns building control systems in about 1,500 FPS-protected facilities that are part of the nation's critical infrastructure, it is

vital that these systems are assessed in a manner that is fully consistent with FISMA and its implementation guidelines.

Recommendations for Executive Action

First, we recommend that the Secretary of Homeland Security, in consultation with GSA, develop and implement a strategy to address cyber risk to building and access control systems that, among other things:

- defines the problem;
- identifies roles and responsibilities;
- analyzes the resources needed; and
- identifies a methodology for assessing this cyber risk.

Second, we recommend that the Secretary of Homeland Security direct ISC to incorporate the cyber threat to building and access control systems into ISC's list of undesirable events in its *Design-Basis Threat* report.

Third, we recommend that the Administrator of the General Services Administration assess the building and access control systems that it owns in FPS-protected facilities in a manner that is fully consistent with FISMA and its implementation guidelines.

Agency Comments

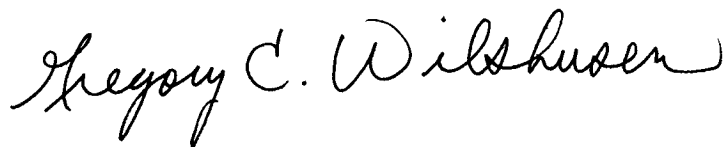
We provided copies of a draft of this report to DHS and GSA for their review and comment. DHS provided written comments, reprinted in appendix III, agreeing with the report's recommendations. DHS also provided technical comments, which we incorporated as appropriate. GSA provided written comments, reprinted in appendix IV, agreeing with the report's recommendations.

As arranged with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this report. At that time, we will send copies of this report to the Secretary of Homeland Security, the Director of the Federal Protective Service, the Administrator the General Services Administration, the Director of the Office of Management and Budget, and other interested parties. The report will also be available on the GAO website at no charge at <http://www.gao.gov>

If you or your staff have any questions about this report, please contact Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.



Mark L. Goldstein
Director, Physical Infrastructure Issues



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objective, Scope, and Methodology

Our objective was to review the extent to which the Department of Homeland Security (DHS) and other stakeholders are prepared to address cyber risks to systems in facilities protected by the Federal Protective Service (FPS).

To perform this work, we reviewed DHS's and other stakeholders' authorities to protect federal facilities. We also reviewed DHS's risk assessment tools; the Interagency Security Committee's guidance and standards on securing federal facilities; and the National Institute of Standards and Technology's cybersecurity guidelines and standards. We also interviewed DHS and FPS headquarters officials about actions being taken and future plans to address cyber risk to systems.

We visited five FPS-protected facilities in the Washington, D.C., area to determine what FPS and other stakeholders were doing to assess and mitigate cyber threats to systems. We determined that there were a sufficient number of facilities in the Washington, D.C., area to represent different types of ownership, different security levels,¹ and uses. Three of the five facilities were government-owned and two were leased from private owners. In addition, one was a multi-tenant facility where we interviewed four tenants and the facility security committee. We also selected facilities housing tenants with different missions, including an agency with research laboratories. At these facilities, we interviewed facility security and information security officials from the General Services Administration (GSA), tenant agencies, and facility owners if they were leased facilities. We also visited an FPS MegaCenter, which is responsible for monitoring alarms from and maintaining communications with field locations, to determine what steps were being taken to secure systems in that facility. The findings from these site visits are not generalizable to all FPS-protected facilities.

We also reviewed GSA's security assessment procedures and a sample of GSA's security assessment reports on building systems, and discussed

¹Tenants determine facility security levels in accordance with ISC's *Risk Management Process for Federal Facilities*. Every nonmilitary facility owned or leased by the federal government is rated from one (lowest level) to five (highest level) based on these factors: facility size, facility population, mission criticality, symbolism, and threat to tenant agencies. We visited three level four facilities, one level three facility, and one level two facility.

them with agency information technology officials. The findings from those reviews are not generalizable to all of GSA's assessment reports.

We reviewed the report of the National Protection and Programs Directorate's (NPPD) pilot combined cyber and physical security assessment and reviewed and discussed the assessment methodologies used with officials in various NPPD components. Furthermore, we collected and analyzed data from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) on cyber incident reports from fiscal year 2010 to fiscal year 2014, and discussed them with the Director of ICS-CERT. ICS-CERT also provided information about the steps that it took to ensure the completeness and reliability of these data, which we determined were sufficiently reliable for our purposes.

To obtain information about the extent to which systems are vulnerable to cyber attacks and the possible consequences, we interviewed DHS officials and experts and reviewed literature and reports. We selected 10 experts from academia and the private sector with relevant experience. These experts were selected through our research, a previous cybersecurity review, and referrals from other experts. The experts' views are not generalizable, but provided a range of perspectives on securing these systems.

We conducted this performance audit from November 2013 through December 2014 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Sources of Cyber-Based Threats and Types of Exploits

Table 2: Sources of Cyber-Based Threats

Threat source	Description
Bot-network operators	Bot-net operators use a network of compromised, remotely controlled systems, referred to as a bot-net, to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Business competitors	Companies that compete against or do business with a target company may seek to obtain sensitive information to improve their competitive advantage in various areas, such as pricing, manufacturing, product development, and contracting.
Criminal groups	Organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Insiders	A disgruntled or corrupt organization insider is a source of computer crime. The insider may not need a great deal of knowledge about computer intrusions because his or her knowledge of a target system is sufficient to allow unrestricted access to cause damage to the system or to steal system data. The insider threat includes malicious current and former employees and contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. A phisher may also use spam and spyware or malware to accomplish their objectives.
Spammers	An individual or organization that distributes unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware.
Terrorists	A terrorist seeks to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. The terrorist may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, National Institute of Standards and Technology, and the Software Engineering Institute's CERT® Coordination Center. | GAO-15-6

**Appendix II: Sources of Cyber-Based Threats
and Types of Exploits**

Table 3: Types of Exploits

Type of exploit	Description
Denial of service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial of service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Trojan Horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use an e-mail program to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Worms	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread. Unlike a computer virus, a worm does not require human involvement to propagate.
Exploits affecting the information security supply chain	The installation of hardware or software that contains malicious logic (like a logic bomb, Trojan Horse, or a virus) or an unintentional vulnerability (the result of an existing defect, such as a coding error) or that may be counterfeited. A supply chain threat can also come from a failure or disruption in the production of a critical product, or a reliance on a malicious or unqualified service provider for the performance of technical services.

Source: GAO analysis of unclassified government and nongovernment data. | GAO-15-6

Appendix III: Comments from the Department of Homeland Security

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



**Homeland
Security**

November 7, 2014

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

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Re: Draft Report GAO-15-6, "FEDERAL FACILITY SECURITY: DHS Should Address Cyber Risk to Building and Access Control Systems"

Dear Messrs. Goldstein and Wilshusen:

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 GAO's positive acknowledgement of the preliminary steps DHS has taken, led by the National Protection and Programs Directorate (NPPD), to begin to understand the cyber risk to building and access control systems. DHS is committed to collaborating with its public, private, and international partners to secure cyberspace and America's cyber assets to safeguard critical infrastructure systems from cyber threats and attacks.

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

Recommendation 1: In consultation with GSA, develop and implement a strategy to address cyber risk to building and access control systems that, among other things:

- defines the problem;
- identifies the roles and responsibilities;
- analyzes the resources needed; and
- identifies a methodology for assessing this cyber risk.

Response: Concur. NPPD's Federal Protective Service and Office of Infrastructure Protection (IP) and Office of Cybersecurity and Communications will consult with GSA, the Interagency Security Committee (ISC) and other relevant federal agencies to develop a strategy for addressing cyber risk to building and access control systems. This strategy will utilize best practices and lessons learned from the private sector experiences of the National Cybersecurity and Communications Integration Center's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Estimated Completion Date (ECD): May 29, 2015.

Recommendation 2: Direct ISC to incorporate the cyber threat to building and access control systems into ISC's list of undesirable events in its *Design-Basis Threat* report.

Response: Concur. As cited in the report, "federal facilities are part of the nation's critical infrastructure (and) determining the extent to which building and access control systems within them are vulnerable to cyber-attacks is critical to providing security." The ISC, which is chaired by the DHS Assistant Secretary of Infrastructure Protection and is composed of Chief Security Officers and other senior executives from 54 Federal departments and agencies, is working with NPPD's United States Computer Emergency Readiness Team and ICS-CERT to incorporate potential cyber risks to buildings and access control systems into the Design-Basis Threat Report and Countermeasures Appendix.

Since protecting federal facilities is a government-wide responsibility, NPPD will work through the ISC to ensure that GSA, federal departments and agencies, and other partners proactively identify and mitigate cybersecurity risks to federal buildings and access control systems. As a next step, the ISC will convene with GSA and other agencies to plan for initial review of cyber risks to building access control and will issue additional guidance to its federal partners on appropriate countermeasures in the next annual review of the Design-Basis Threat Report. ECD: October 30, 2015.

Again, thank you for the opportunity to review and provide 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, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Appendix IV: Comments from the General Services Administration



The Administrator

November 26, 2014

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the draft report, "Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems" (GAO-15-6). The U.S. Government Accountability Office (GAO) recommends that GSA assess cyber risk of its building control systems in a manner that fully reflects FISMA and its guidelines.

GSA agrees with the findings and the recommendations and will take appropriate action to ensure its assessments of the cyber risks of its building control systems are conducted in a manner that fully reflects FISMA and implementing guidelines. In addition, GSA will partner with the Department of Homeland Security to develop and implement a framework for these cyber risks.

If you have any additional questions or concerns, please feel free to contact me at (202) 501-0800, or Ms. Lisa A. Austin, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "Dan Tangherlini".

Dan Tangherlini
Administrator

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405
Telephone: (202) 501-0800
Fax: (202) 219-1243

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contacts

Mark L. Goldstein, (202) 512-2934 or goldsteinm@gao.gov
Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact named above, Tammy Conquest, Assistant Director; John de Ferrari, Assistant Director; Geoff Hamilton, Bob Homan, Thomas Johnson, Seth Malaguerra, and SaraAnn Moessbauer made key contributions to this report.

Related GAO Products

Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity. [GAO-14-459](#). Washington, D.C.: June 5, 2014.

Information Security: Agencies Need to Improve Cyber Incident Response Practices. [GAO-14-354](#). Washington, D.C.: April 30, 2014.

Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness. [GAO-13-776](#). Washington, D.C.: September 26, 2013.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. [GAO-13-187](#). Washington, D.C.: February 14, 2013.

Cybersecurity: Threats Impacting the Nation. [GAO-12-666T](#). April 24, 2012.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. [GAO-11-865T](#). Washington, D.C.: July 26, 2011.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. [GAO-08-526](#). Washington, D.C.: May 21, 2008.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. [GAO-07-1036](#). Washington, D.C.: September 10, 2007.

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 (<http://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 <http://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, <http://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 www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

