United States Government Accountability Office

Report to Congressional Requesters

May 2016

INFORMATION SECURITY

Agencies Need to Improve Controls over Selected High-Impact Systems

GAO-16-501

GAO Highlights

Highlights of GAO-16-501, a report to congressional requesters

May 2016

INFORMATION SECURITY

Agencies Need to Improve Controls over Selected High-Impact Systems

Why GAO Did This Study

Federal systems categorized as high impact—those that hold sensitive information, the loss of which could cause individuals, the government, or the nation catastrophic harm—warrant increased security to protect them. In this report, GAO (1) describes the extent to which agencies have identified cyber threats and have reported incidents involving high-impact systems, (2) identifies government-wide guidance and efforts to protect these systems, and (3) assesses the effectiveness of controls to protect selected high-impact systems at federal agencies. To do this, GAO surveyed 24 federal agencies; examined federal policies, standards, guidelines and reports; and interviewed agency officials. In addition, GAO tested and evaluated the security controls over eight high-impact systems at four agencies.

What GAO Recommends

GAO recommends that OMB complete its plans and practices for securing federal systems and that NASA, NRC, OPM, and VA fully implement key elements of their information security programs. The agencies generally concurred with GAO's recommendations, with the exception of OPM. OPM did not concur with the recommendation regarding evaluating security control assessments. GAO continues to believe the recommendation is warranted.

In separate reports with limited distribution, GAO is making specific recommendations to each of the four agencies to mitigate identified weaknesses in access controls, patch management, and contingency planning.

View GAO-16-501. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

In GAO's survey of 24 federal agencies, the 18 agencies having high-impact systems identified cyber attacks from "nations" as the most serious and most frequently-occurring threat to the security of their systems. These agencies also noted that attacks delivered through e-mail were the most serious and frequent. During fiscal year 2014, 11 of the 18 agencies reported 2,267 incidents affecting their high-impact systems, with almost 500 of the incidents involving the installation of malicious code.

Government entities have provided guidance and established initiatives and services to aid agencies in protecting their systems, including those categorized as high impact. The National Institute of Standards and Technology has prescribed federal standards for minimum security requirements and guidance on security and privacy controls for high-impact systems, including 83 controls specific to such systems. The Office of Management and Budget (OMB) is developing plans for shared services and practices for federal security operations centers but has not issued them yet. In addition, agencies reported that they are in the process of implementing various federal initiatives, such as tools to diagnose and mitigate intrusions on a continuous basis and stronger controls over access to agency networks.

The National Aeronautics and Space Administration (NASA), Nuclear Regulatory Commission (NRC), Office of Personnel Management (OPM), and Department of Veterans Affairs (VA) had implemented numerous controls over the eight high-impact systems GAO reviewed. For example, all the agencies reviewed had developed a risk assessment for their selected high-risk systems. However, the four agencies had not always effectively implemented access controls. These control weaknesses included those protecting system boundaries, identifying and authenticating users, authorizing access needed to perform job duties, and auditing and monitoring system activities. Weaknesses also existed in patching known software vulnerabilities and planning for contingencies. An underlying reason for these weaknesses is that the agencies had not fully implemented key elements of their information security programs, as shown in the table.

Agency Implementation of Key Information Security Program Elements for Selected Systems

	NASA	NRC	OPM	VA
Risk assessments	●	●	●	●
Security plans	●	◐	◐	◐
Controls assessments	◐	◐	◐	○
Remedial action plans	◐	◐	◐	◐

Source: GAO analysis of agency documentation. | GAO-16-501

Note: ● – Met ◐ – Partially met ○ – Did not meet

Until the selected agencies address weaknesses in access and other controls, including fully implementing elements of their information security programs, the sensitive data maintained on selected systems will be at increased risk of unauthorized access, modification, and disclosure, and the systems at risk of disruption.

Contents

Figures

Abbreviations

Agriculture	U.S. Department of Agriculture
C-CAR	Federal Cybersecurity Coordination, Assessment, and Response
CDM	Continuous Diagnostics and Mitigation
Commerce	Department of Commerce
Defense	Department of Defense
DHS	Department of Homeland Security
Education	Department of Education
Energy	Department of Energy
EPA	Environmental Protection Agency
FIPS Pub	*Federal Information Processing Standard* Publication
FISMA	*Federal Information Security Modernization Act of 2014*
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
Interior	Department of the Interior
ISIMC	Information Security and Identity Management Committee
Justice	Department of Justice
Labor	Department of Labor
NASA	National Aeronautics and Space Administration
NCPS	National Cybersecurity Protection System
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIV	personal identity verification
POA&M	plan of action and milestones
SBA	Small Business Administration
SSA	Social Security Administration
State	Department of State
TIC	Trusted Internet Connections
Transportation	Department of Transportation
Treasury	Department of the Treasury
USAID	U.S. Agency for International Development
US-CERT	United States Computer Emergency Readiness Team
VA	Department of Veterans Affairs

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

May 18, 2016

The Honorable Ron Johnson
Chairman
The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan M. Collins
United States Senate

The breach at the Office of Personnel Management (OPM), reported in July 2015, affected at least 21.5 million individuals and demonstrates the catastrophic effect that such an incident can have on an agency's mission and national security. Increasingly sophisticated threats to information technology systems and the damage that can be generated underscore the importance of managing and protecting them. This is particularly true for those systems agencies categorize as high impact, where the loss of confidentiality, integrity, or availability can have a severe or catastrophic adverse effect on organizational operations, assets, or individuals. Such an impact can result in loss or degradation of mission capability, severe harm to individuals, or major financial loss. Having government-wide guidance, initiatives, and services in place is important for their protection.

Since 1997, we have designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure.[1] Most recently, in the February 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information.[2]

[1]See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[2]Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

In response to your request, we reviewed the security over federal high-impact systems. Our objectives were to 1) describe the extent to which agencies have identified cyber threats and reported incidents involving high-impact systems; 2) identify government-wide guidance and efforts to protect these systems; and 3) assess the effectiveness of controls to protect selected high-impact systems at selected federal agencies.

We surveyed the 24 federal agencies[3] covered by the *Chief Financial Officers Act* [4] to collect, analyze, and summarize data on the cyber threats, security incidents, and security guidance and efforts involving high-impact systems. We also examined federal policies, standards, guidelines, reports, and other artifacts issued by organizations with government-wide information security responsibilities, such as the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST)[5] and the Department of Homeland Security (DHS), and interviewed officials at these organizations regarding actions to provide guidance and services to protect federal systems.

In addition, we selected four agencies—the Department of Veterans Affairs (VA), the National Aeronautics and Space Administration (NASA), OPM, and the Nuclear Regulatory Commission (NRC)—for testing controls over selected systems.[6] At each of these four agencies, we selected two systems for which the impact of a compromise to each of the

[3]The 24 departments and agencies covered by the *Chief Financial Officers Act* are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[4]31 U.S.C. § 901.

[5]The National Institute of Standards and Technology is part of the Department of Commerce.

[6]We ranked the 24 agencies based on the number of high-impact systems the agency reported to OMB in fiscal year 2014 from the most to least number of high-impact systems, then divided the list into quartiles and selected the first agency in each quartile. We subtracted any national security systems that had been included in agency reporting before ranking the agencies from highest to lowest. We also removed any agency that did not report any high impact systems before dividing the list into quartiles.

three security objectives of confidentiality, integrity, and availability[7] was categorized as "high," as reported to us by the agency. Further, to determine the effectiveness of controls over selected systems at the four agencies, we reviewed and analyzed documents, including information security policies, plans, and procedures; reviewed the testing of controls and performed tests of selected controls over the systems; and interviewed agency officials. See appendix I for additional details on our objectives, scope, and methodology.

We conducted this performance audit from February 2015 to May 2016 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.

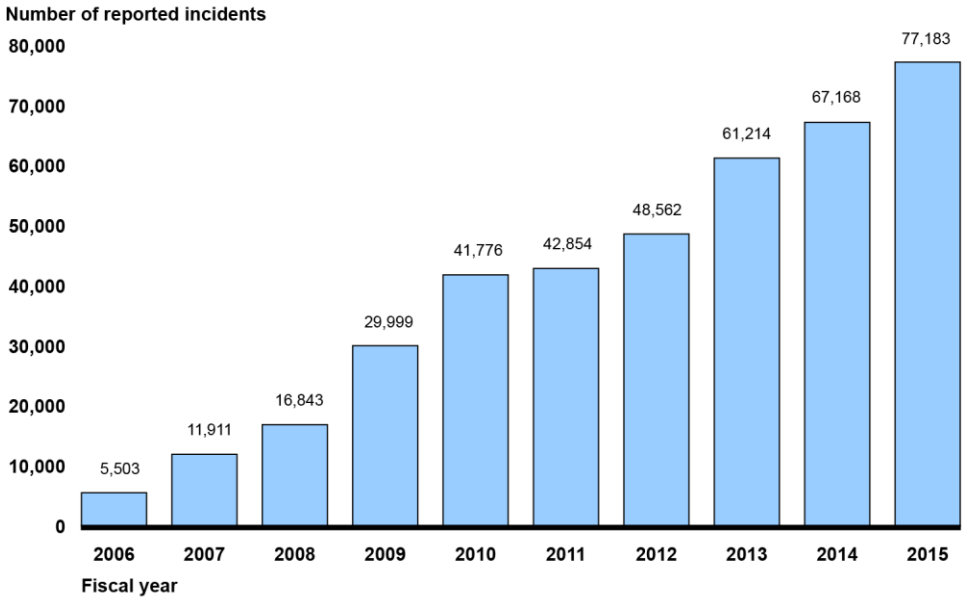
Background

The federal government faces various cyber-based threats to its systems and data, as reported by federal agencies to the United States Computer Emergency Readiness Team (US-CERT).[8] Indeed, the number of information security incidents affecting systems supporting the federal government has continued to increase. Since fiscal year 2006, the number has risen from 5,503 to 77,183 in fiscal year 2015, an increase of about 1,303 percent. Figure 1 illustrates the increasing number of security incidents at federal agencies from 2006 through 2015.

[7]NIST describes a loss of confidentiality as the unauthorized disclosure of information, a loss of integrity as the unauthorized modification or destruction of information, and a loss of availability as the disruption of access to or use of information or an information system.

[8]US-CERT, a component of DHS, operates the federal information security incident center.

Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-501

These incidents and others like them can pose a serious challenge to economic, national, and personal privacy and security. Recent examples highlight the impact of such incidents:

- In June 2015, the Commissioner of Internal Revenue testified that unauthorized third parties had gained access to taxpayer information from its “Get Transcript” application. According to officials, criminals used taxpayer-specific data acquired from non-agency sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included Social Security information, dates of birth, and street addresses. In an August 2015 update, the Internal Revenue Service reported this number to be about 114,000, and said that an additional 220,000 accounts had been inappropriately accessed. In February 2016, the agency reported the potential access of approximately 390,000 additional taxpayer accounts during the period from January 2014 through May 2015. Thus, about 724,000 accounts were reportedly affected. The online Get Transcript service has been unavailable since May 2015.

- In June 2015, OPM reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate but related incident had affected background investigation files and compromised its systems related to background investigations for 21.5 million individuals.
- According to a VA official, in January 2014, a software defect in its eBenefits system had improperly allowed users to view the personal information of other veterans. According to this official, this defect had the potential to allow almost 5,400 users to view data of more than 1,300 veterans and/or their dependents.

Federal Law Establishes Information Security Requirements to Protect Federal Systems

The *Federal Information Security Modernization Act* (FISMA) of 2014[9] provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and for ensuring the effective oversight of information security risks, including those throughout civilian, national security, and law enforcement agencies. The law requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency. Such a program includes assessing risks; developing and implementing policies and procedures to cost-effectively reduce risks; plans for providing adequate information security for networks, facilities, and systems; providing security awareness and specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; procedures for detecting, reporting, and responding to security incidents; and ensuring continuity of operations.

FISMA also establishes key government-wide roles for OMB, DHS, and NIST. These include the following:

[9]The *Federal Information Security Modernization Act of 201*4 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) partially superseded *The Federal Information Security Management Act of 2002* (FISMA 2002), enacted as title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

- **OMB**—OMB is required to update data breach notification policies and guidelines periodically, and provide in its annual report to Congress a summary of major information security incidents and an assessment of each agency's compliance with NIST standards and breach notification requirements, among other things. Further, OMB is required to work in consultation with DHS in developing guidance to evaluate the effectiveness of agencies' information security programs and practices.
- **DHS**—FISMA includes requiring DHS to assist OMB with providing oversight by administering the implementation of information security policies and practices for information systems. Key DHS responsibilities include developing and overseeing the implementation of binding operational directives requiring agencies to implement OMB's information security standards and guidelines; operating a federal information security incident center (US-CERT); and, on request by an agency, deploying technology to assist the agency to continuously diagnose and mitigate cyber threats and vulnerabilities.
- **NIST**—NIST develops standards and guidelines that include minimum information security requirements to protect federal systems.

NIST Defines How Agencies Categorize System Impact Levels and Select Controls Necessary to Protect Systems Based on Impact Level

NIST Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (FIPS Pub 199) defines how agencies should determine the security category of their information and information systems.[10] Agencies are to consider the potential impact or magnitude of harm that could occur should there be a loss in the confidentiality, integrity, or availability of the information or information system as low, moderate, or high.

1. Low impact: The loss could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. For example, the loss might cause degradation in an organization's mission capability to an extent and duration that the organization is able to perform its functions, but the effectiveness of the functions is noticeably reduced.

[10]National Institute of Standards and Technology, *Federal Information Processing Standards Publication Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199, (Gaithersburg, MD: February 2004).

2. Moderate impact: The loss could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. The loss could significantly reduce the agency's capability to effectively perform its mission and functions, among other things.
3. High impact: The loss could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. For example, it might cause the organization to be unable to perform one or more of its primary functions or result in a major financial loss.

Agencies are to determine an impact level for each of the three security objectives of confidentiality, integrity, and availability for the information types within a system.

NIST prescribes that the security category of an information system shall be the highest impact level (i.e., high water mark) that was determined for the three security objectives. A system is categorized as high impact when the impact of the loss of at least one of the three security objectives—confidentiality, integrity, or availability—is determined to be high. For example, if an agency considered loss of confidentiality as high impact, and loss of availability and integrity as low, the security category for the system would be considered as high impact.

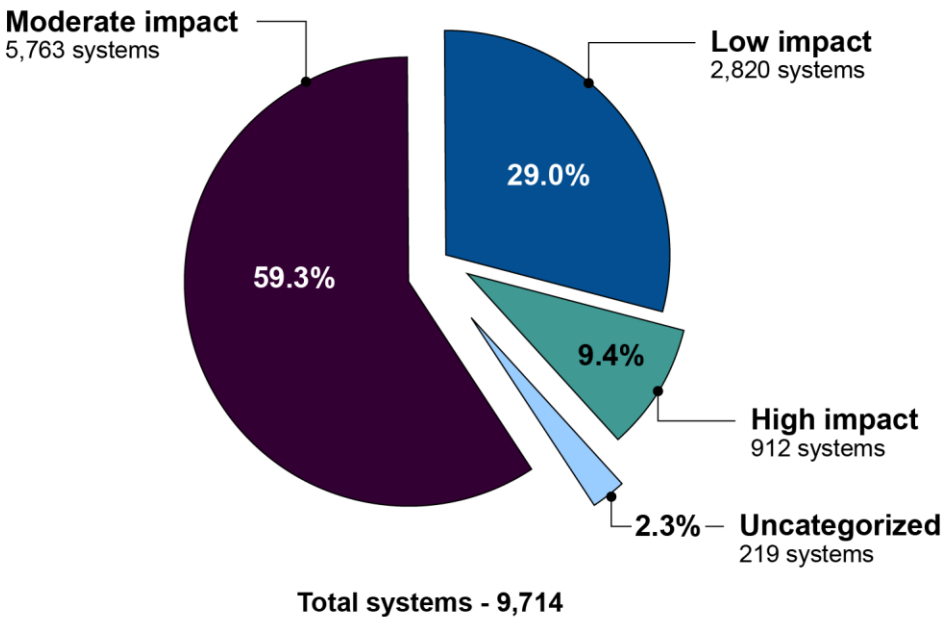
To assist agencies in implementing the appropriate information security controls, NIST FIPS Pub 200 specifies minimum security requirements for federal information and information systems.[11] Minimum security requirements are based in part on system impact levels and provide for a greater baseline of information security controls for high-impact systems than they do for moderate- and low-impact systems. A greater baseline is warranted because, if a high-impact system is attacked or compromised, the consequences would likely be more catastrophic than those of a moderate- or low-impact system.

In fiscal year 2015, the 24 agencies covered by the *Chief Financial Officers Act* reported having 912 high-impact systems, or about 9 percent

[11]National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Pub 200, (Gaithersburg, MD: March 2006).

of the 9,714 systems they reported to OMB, as part of the agencies' FISMA reporting requirements, as shown in figure 2.

Figure 2: Categorization of Impact Level for Federal Systems in Fiscal Year 2015



Source: GAO analysis of agency fiscal year 2015 data. | GAO-16-501

Agencies Have Identified a Variety of Cyber Threats and Incidents, Some More Serious and Prevalent than Others

Agencies have identified the most serious and most often occurring threats, as well as incidents affecting their high-impact systems. We surveyed the 24 *Chief Financial Officers Act* agencies, and 18 reported having one or more high-impact system.[12] In response to our questions, each of the 18 agencies identified what they considered to be their top three threat sources, means of attack, and attack methods that they consider to be the most serious and most frequently occurring to high-impact systems. Agencies also commented on the extent to which resources provided by federal entities have assisted them in identifying cyber threats and noted several challenges they have encountered in doing so. Further, agencies reported on incidents affecting their high-impact systems.

Adversarial Threat Sources Have Employed Numerous Attack Methods through Various Means

Adversarial threat sources are individuals, groups, organizations, or nations that seek to exploit the target organization's dependence on cyber resources (i.e., information in electronic form, information and communication technologies, and the communications and information-handling capabilities provided by those technologies). See table 1 for a listing of adversarial threat sources.

[12]The 18 agencies reporting high-impact systems are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, the Interior, Justice, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, Nuclear Regulatory Commission, and Office of Personnel Management. The following six agencies reported having no high-impact systems: the Departments of Housing and Urban Development and Labor, as well as the National Science Foundation, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

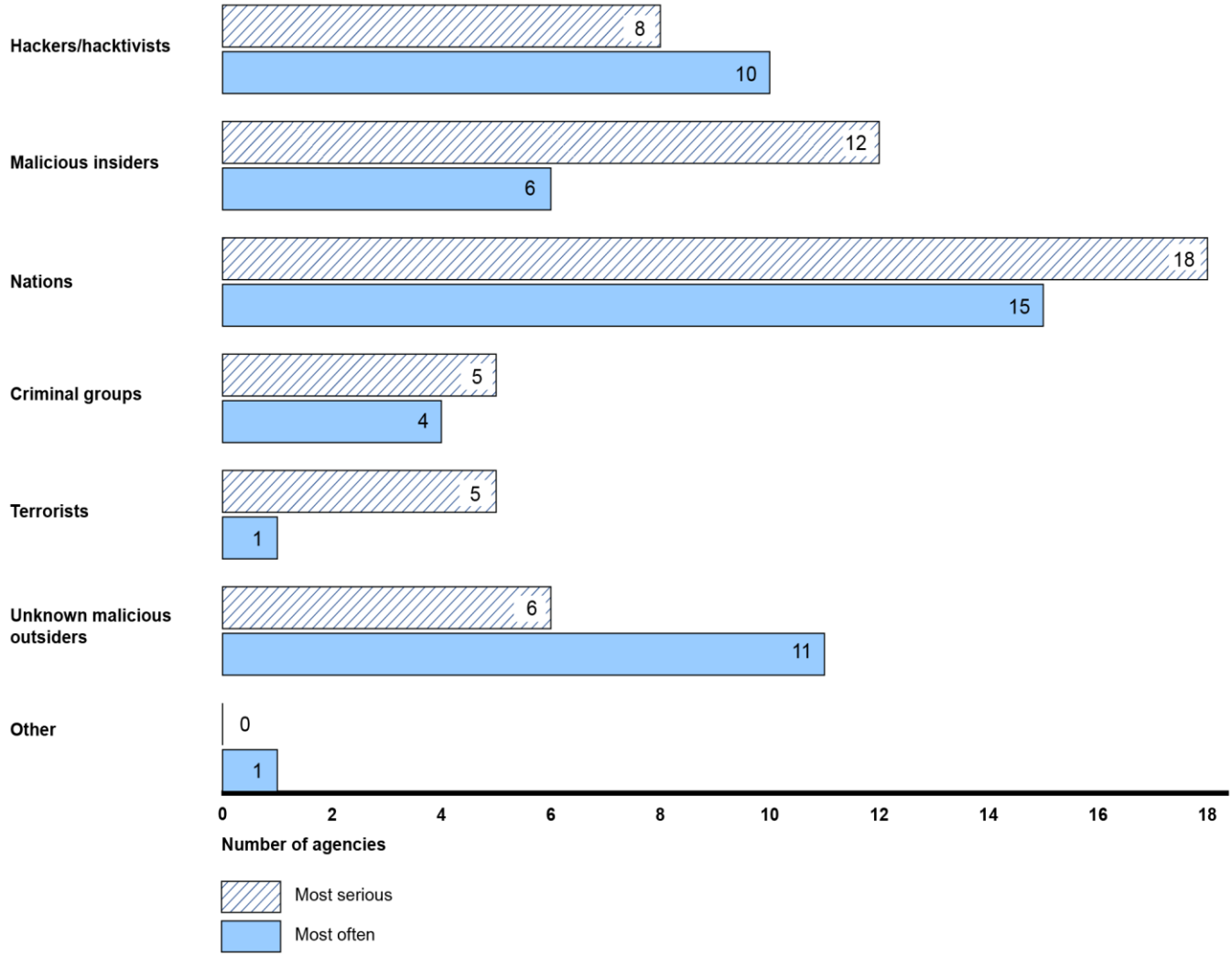
Table 1: Adversarial Cyber Threat Sources

Adversarial source	Description
Hacker/hacktivist	Hackers break into networks for challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals.
Malicious insiders	Insiders (e.g., disgruntled organization employees, including contractors) may not need a great deal of knowledge about computer intrusions because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. These individuals engage in purely malicious activities and should not be confused with non-malicious insider accidents.
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned programs use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities.
Criminal groups and organized crime	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion.
Terrorists	Terrorists seek 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.
Unknown malicious outsiders	Unknown malicious outsiders are threat sources that, due to a lack of information, remain anonymous and are unable to be classified as one of the five types of threat sources listed.

Source: GAO analysis of government and nongovernment data. | GAO-16-501.

Figure 3 shows the adversarial threats agencies selected as being the most frequent and the most serious. Agencies reported that nations and malicious insiders were the most serious threats, and that nations, unknown malicious outsiders, and hackers/hacktivist threats occurred most often, as indicated, for example, by alerts or notifications.

Figure 3: Most Serious and Most Frequently Identified Adversarial Cyber Threat Sources/Agents, as Reported by 18 Agencies with High-Impact Systems



Source: GAO summary based on responses to GAO survey. | GAO-16-501

In carrying out a system attack, adversarial threat agents can use a variety of methods and exploits, as described in table 2.

Table 2: Common Cyber Threat Attack Methods and Exploits

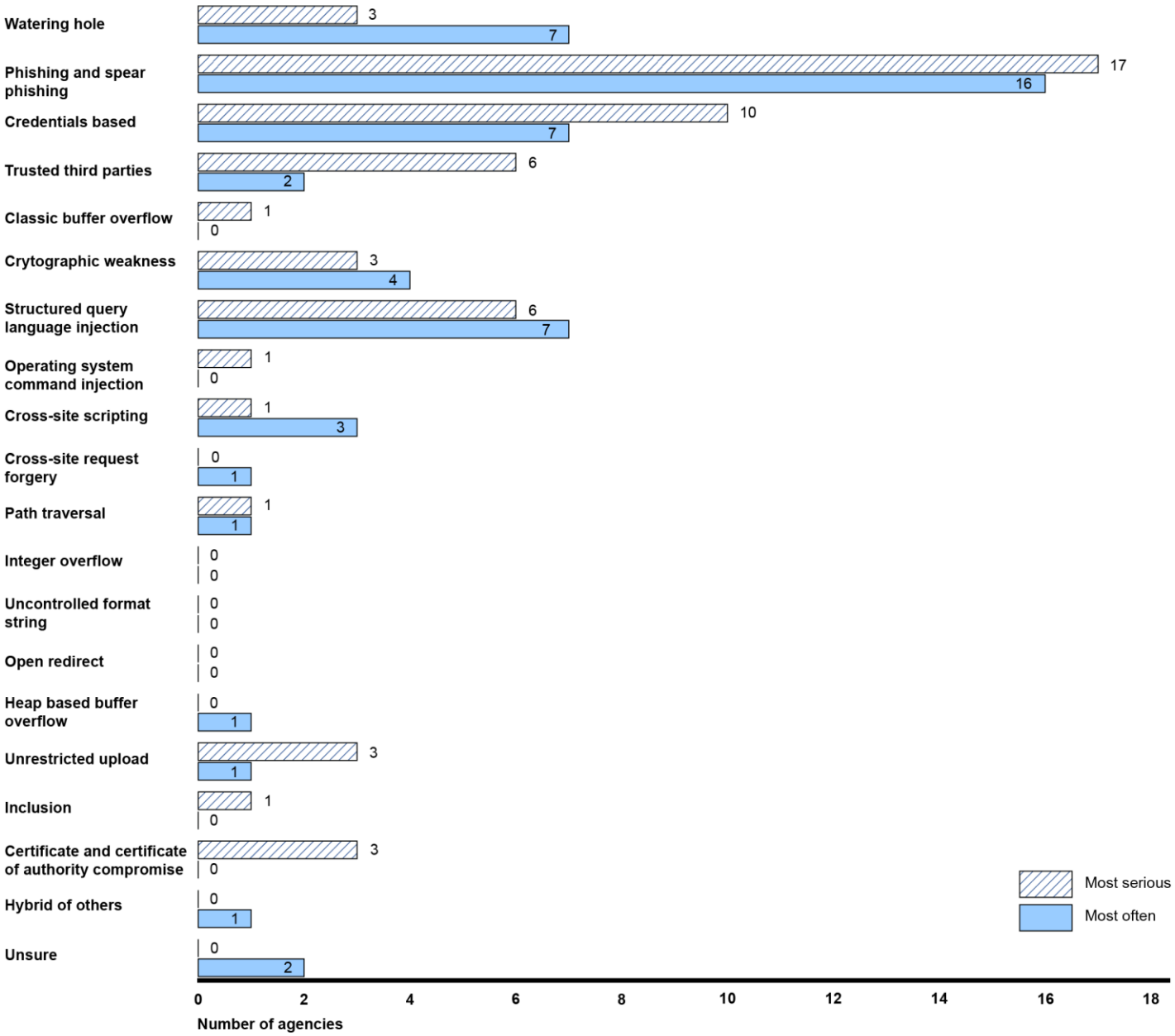
Method of exploit	Description
Watering hole	A method by which threat actors exploit the vulnerabilities of websites frequented by users of the targeted system. Malware is then injected to the targeted system via the compromised websites.
Phishing & spear phishing	A digital form of social engineering that uses authentic-looking e-mails, websites, or instant messages to get users to download malware, open malicious attachments, or open links that direct them to a website that requests information or executes malicious code.
Credentials based	An exploit that takes advantage of a system's insufficient user authentication and/or any elements of cybersecurity supporting it, to include not limiting the number of failed login attempts, the use of hard-coded credentials, and the use of a broken or risky cryptographic algorithm.
Trusted third parties	An exploit that takes advantage of the security vulnerabilities of trusted third parties to gain access to an otherwise secure system.
Classic buffer overflow	An exploit that involves the intentional transmission of more data than a program's input buffer can hold, leading to the deletion of critical data and subsequent execution of malicious code.
Cryptographic weakness	An exploit that takes advantage of a network employing insufficient encryption when either storing or transmitting data, enabling adversaries to read and/or modify the data stream.
Structured Query Language (SQL) injection	An exploit that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database resulting in data loss or corruption, denial of service, or complete host takeover.
Operating system command injection	An exploit that takes advantage of a system's inability to properly neutralize special elements used in operating system commands, allowing adversaries to execute unexpected commands on the system by either modifying already evoked commands or evoking their own.
Cross-site scripting	An exploit that uses third-party web resources to run lines of programming instructions (scripts) within the victim's web browser or scriptable application. This occurs when a user, using a browser, visits a malicious website or clicks a malicious link. The most dangerous consequences can occur when this method is used to exploit additional vulnerabilities that may permit an adversary to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, or remotely access and control the victim's machine.
Cross-site request forgery	An exploit that takes advantage of an application that cannot, or does not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request, tricking the victim into executing a falsified request that results in the system or data being compromised.
Path traversal	An exploit that seeks to gain access to files outside of a restricted directory by modifying the directory path name in an application that does not properly neutralize special elements (e.g., '…', '/', '…/') within the path name.
Integer overflow	An exploit where malicious code is inserted that leads to unexpected integer overflow, or wraparound, which can be used by adversaries to control looping or make security decisions in order to cause program crashes, memory corruption, or the execution of arbitrary code via buffer overflow.
Uncontrolled format string	Adversaries manipulate externally controlled format strings in print-style functions to gain access to information and execute unauthorized code or commands.
Open redirect	An exploit where the victim is tricked into selecting a URL (website location) that has been modified to direct them to an external, malicious site that might contain malware that can compromise the victim's machine.
Heap-based buffer overflow	Similar to classic buffer overflow, but the buffer that is overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a memory allocation routine, such as "malloc ()".

Method of exploit	Description
Unrestricted upload of files	An exploit that takes advantage of insufficient upload restrictions, enabling adversaries to upload malware (e.g., .php) in place of the intended file type (e.g., .jpg).
Inclusion of functionality from un-trusted sphere	An exploit that uses trusted, third-party executable functionality (e.g., web widget or library) as a means of executing malicious code in software whose protection mechanisms are unable to determine whether functionality is from a trusted source, modified in transit, or being spoofed.
Certificate and certificate authority compromise	Exploits facilitated via the issuance of fraudulent digital certificates (e.g., transport layer security and Secure Socket Layer). Adversaries use these certificates to establish secure connections with the target organization or individual by mimicking a trusted third party.
Hybrid of others	An exploit that combines elements of two or more of the aforementioned techniques.

Source: GAO analysis of government and nongovernment data. | GAO-16-501.

Agencies reported that they considered phishing and spear phishing (attachment-based and link-based), credentials-based (password reuse, guessing, and brute-force), trusted third parties, and SQL injection as the most serious attack methods in terms of affecting their high-impact systems. They also listed phishing and spear phishing (attachment-based and link-based), watering hole, credentials-based (password reuse, guessing, and brute-force), and SQL injection as the methods that affected their high-impact systems the most often, in terms of notifications or alerts. Figure 4 shows agencies' responses for the most often and most serious methods of cyber attack towards their high-impact systems.

Figure 4: Most Serious and Most Frequently Identified Cyber Attack Methods, as Reported by 18 Agencies with High-Impact Systems



Source: GAO summary based on responses to GAO survey. | GAO-16-501

Further, adversarial threat agents may use various means, or threat vectors, to carry out an attack. A threat vector specifies the conduit or medium used by the threat source to initiate a cyber attack (e.g. attackers may use an e-mail to engage in phishing or spear phishing to steal personally identifiable information). US-CERT's taxonomy of threat vectors is described in table 3.

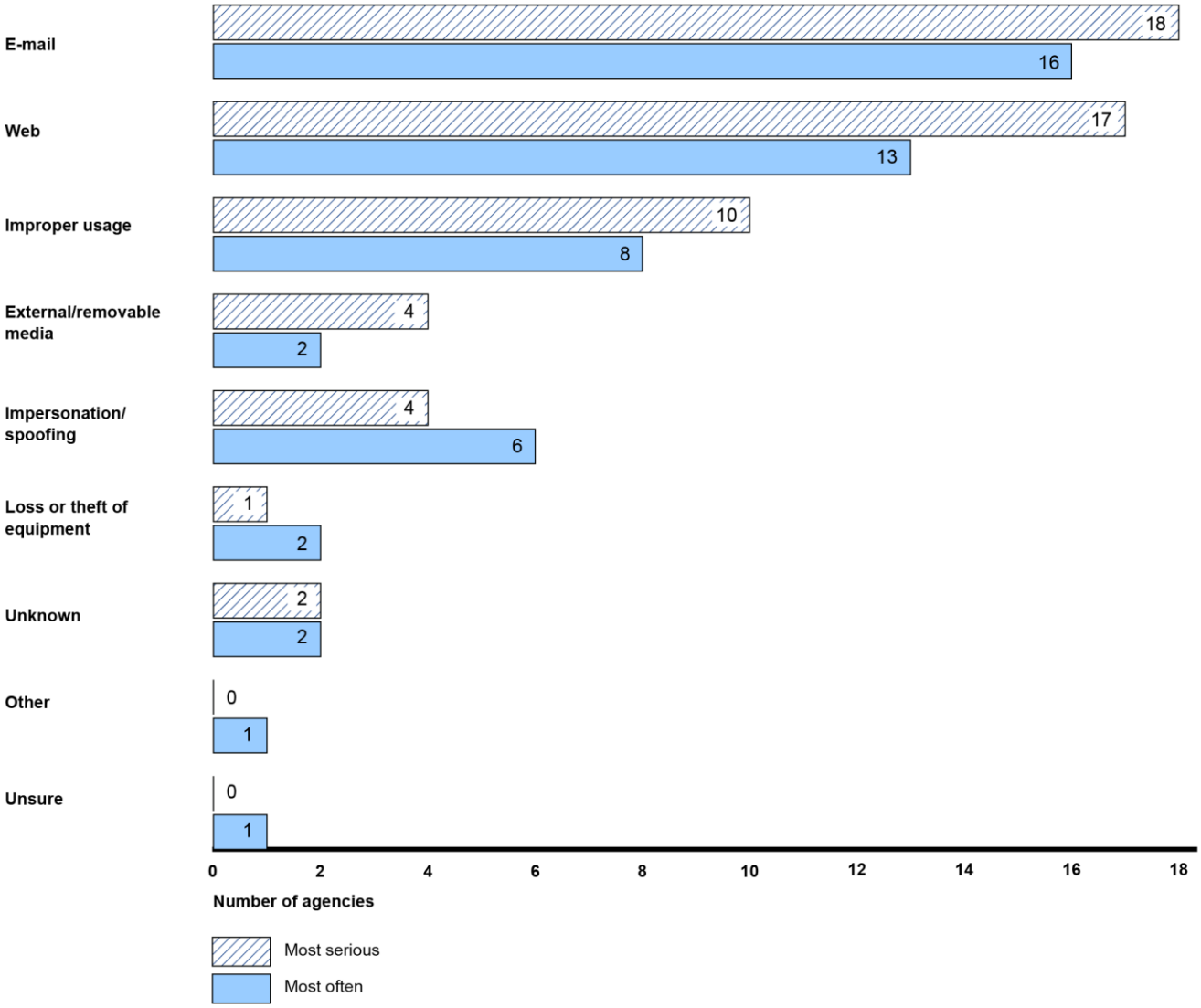
Table 3: Cyber Threat Attack Vectors

Vector	Description	Example
E-mail	An attack executed via an e-mail message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an e-mail message.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Improper usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data or a user performs illegal activities on a system.
External removable media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected USB flash drive.
Impersonation/spoofing	An attack involving replacement of legitimate content/services with a malicious substitute.	Spoofing, man-in-the-middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
Loss or theft of equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown on initial report. The threat vector may be updated in a follow-up report.

Source: List of cyber threat attack vectors developed by US-CERT and made available on their website. I GAO-16-501 .

Agencies indicated that they considered e-mail, Web, and improper usage to be the most serious and most frequently used threat vectors that affect their high-impact systems, as indicated in figure 5.

Figure 5: Most Serious and Most Frequently Identified Cyber Threat Vectors, as Reported by 18 Agencies with High-Impact Systems



Source: GAO summary based on responses to GAO survey. | GAO-16-501

Non-adversarial Threats Can Also Impair System Operations and Data

In addition to adversarial threats, non-adversarial threats could also affect high-impact systems. Non-adversarial threat sources include failures in equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters. They also include natural disasters and failures of critical infrastructure on which the organization depends, but are outside of the control of the organization, and are listed in table 4.

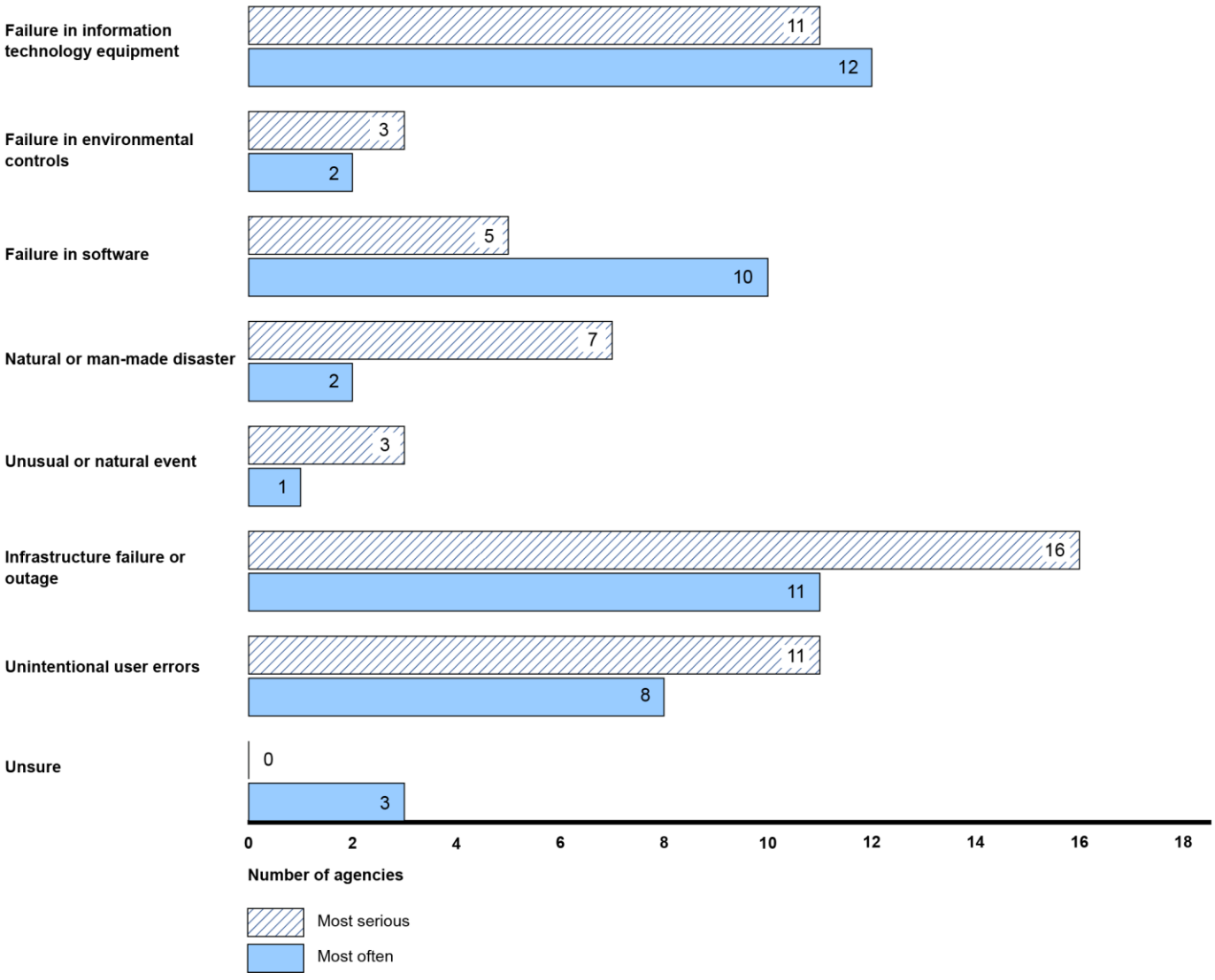
Table 4: Non-adversarial Types of Cyber Threat Sources

Type	Description
Failure in information technology equipment	Failures in displays, sensors, controllers, and information technology hardware responsible for data storage, processing, and communications.
Failure in environmental controls	Failures in temperature/humidity controllers or power supplies.
Failures in software	Failures in operating systems, networking, and general-purpose and mission-specific applications.
Natural or man-made disaster	Events beyond an entity's control such as fires, floods, tsunamis, tornados, hurricanes, and earthquakes.
Unusual or natural event	Natural events beyond the entity's control that are not considered disasters (e.g., sunspots).
Infrastructure failure or outage	Failure or outage of telecommunications or electrical power.
Unintentional user errors	Failures resulting from erroneous accidental actions taken by individuals (both system users and administrators) in the course of executing their everyday responsibilities.

Source: GAO analysis of non-adversarial/non-malicious cyber threat sources published by NIST in NIST SP 800-30. I GAO-16-501.

As shown in figure 6, agencies with high-impact systems reported that they considered infrastructure failure or outage, failure in IT equipment, and unintentional user errors to be the most serious non-adversarial threat sources that affect their high-impact systems. They also indicated that failure in IT equipment, infrastructure failure or outage, and failure in software were the non-adversarial threat sources that most often affect their high-impact systems.

Figure 6: Most Serious and Most Frequently Used Non-adversarial Cyber Threat Sources, as Reported by 18 Agencies with High-Impact Systems

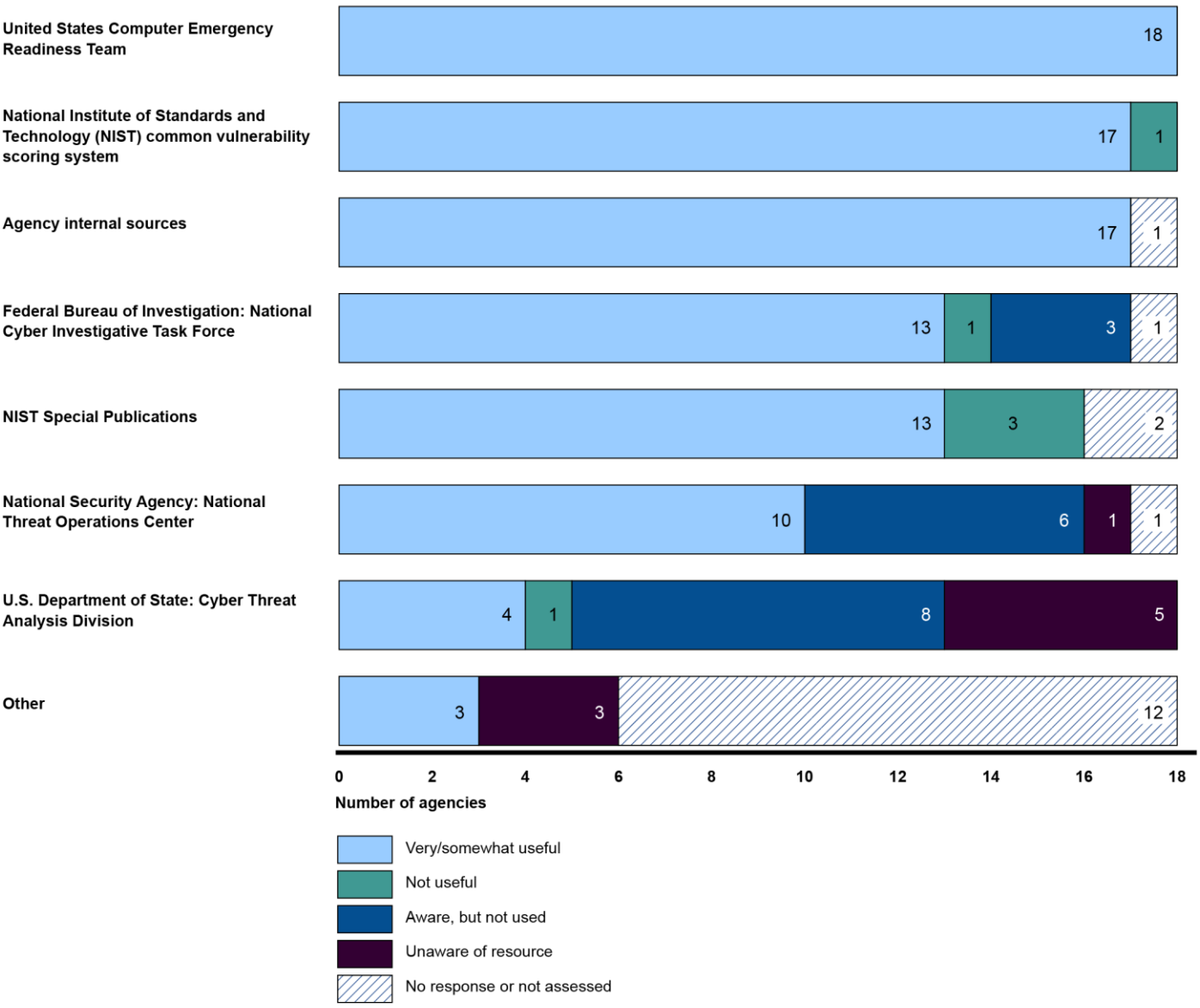


Source: GAO summary based on responses to GAO survey. | GAO-16-501

Agencies Reported Using a Variety of Resources and Encountering Common Challenges in the Identification of Cyber Threats

Agencies reported using a variety of both public and private resources to assist them in identifying potential cyber threats, the use and usefulness of which vary, as shown in figure 7. The most useful of these resources is US-CERT, which was identified by all 18 agencies as being either very or somewhat useful. The second and third most useful resources, both of which were identified by 17 agencies as being either very or somewhat useful, are NIST's Common Vulnerability Scoring System and agency internal sources (e.g., shared services and security operations centers).

Figure 7: Usefulness of Federal Resources in Assisting Agencies in Identifying Cyber Threats, as Reported by 18 Agencies with High-Impact Systems



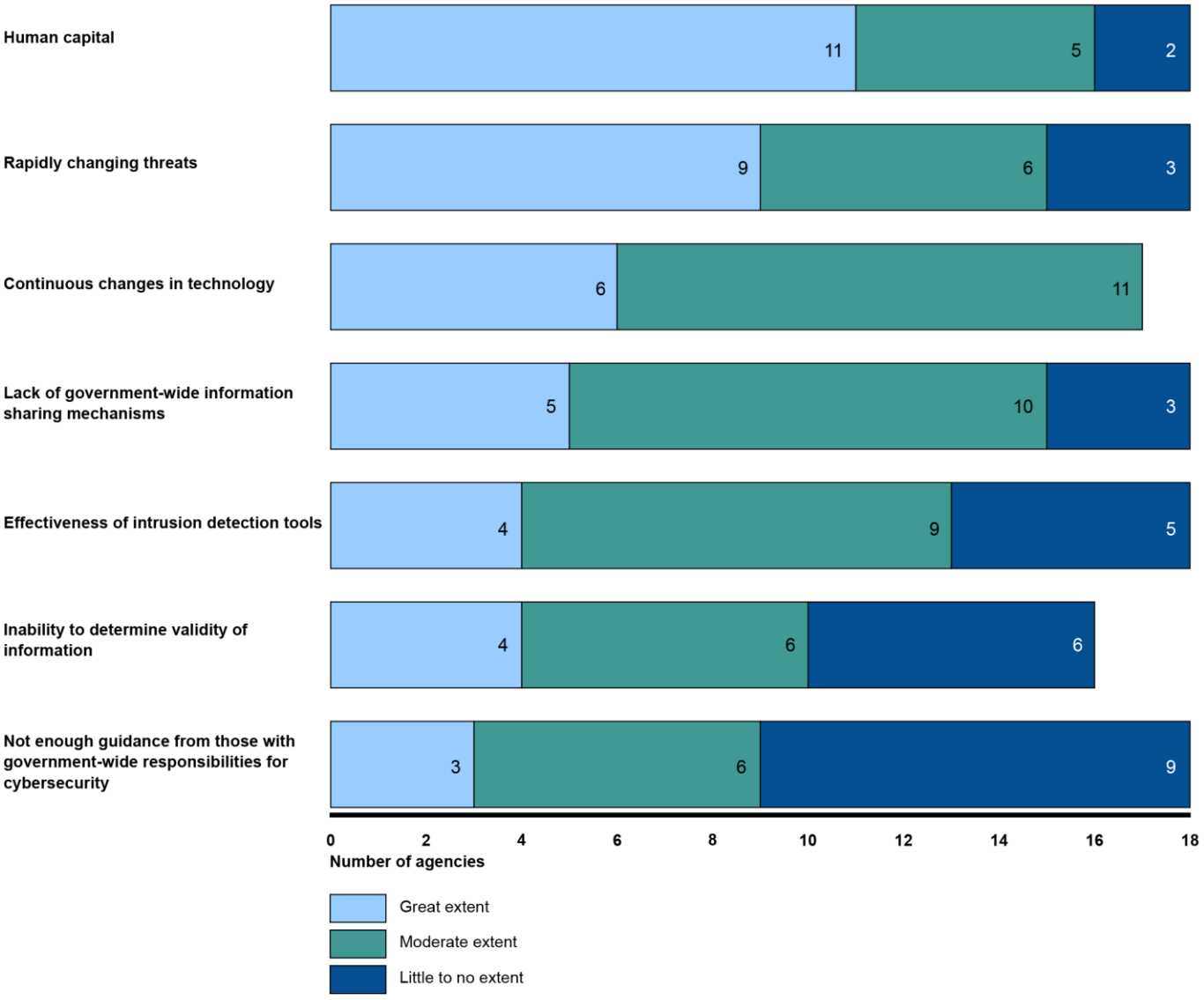
Source: GAO summary based on responses to GAO survey. | GAO-16-501

Agencies Encountered Challenges in Identifying Cyber Threats

Challenges also exist for agencies in effectively identifying threats, as shown in figure 8. For example, in our survey, we asked agencies to identify the extent to which their inability to recruit staff with appropriate skills, the limited effectiveness of intrusion detection devices, and other challenges hinder their ability to identify threats. In their responses, of the 18 agencies with high-impact systems

- 11 noted that human capital (recruiting and retaining personnel with the knowledge, skills, and abilities necessary to perform cybersecurity functions) limited their ability to identify threats to a great extent;
- 9 found rapidly changing threats impaired their ability to identify threats to a great extent;
- 11 noted that continuous changes in technology hindered their ability to identify threats to a moderate extent;
- 10 indicated a lack of government-wide information sharing mechanisms limited their ability to identify threats to a moderate extent; and
- 9 found the limited effectiveness of intrusion detection tools moderately reduced their ability to identify threats.

Figure 8: Challenges Hindering Agencies in Identifying Cyber Threats, as Reported by 18 Agencies with High-Impact Systems



Source: GAO summary based on responses to GAO survey. | GAO-16-501

Agencies Reported Incidents that Affected Their High-Impact Systems

In response to our survey, 14 of 18 agencies responded that their agency experienced cybersecurity incidents that affected their high-impact systems during the period October 2013 through June 2015. We then asked about the specific number of incidents that occurred in fiscal year 2014.

Of the 14 agencies that responded regarding incidents affecting their high-impact systems,

- 11 reported 2,267 incidents affecting their high-impact systems, with one agency accounting for 61 percent of the total and
- 3 did not specify the number of incidents affecting their high-impact systems.

For the remaining 4 agencies, 3 reported that they had no incidents affecting their high-impact systems during the period and one reported "unknown."

Over the last several years, US-CERT has required agencies to categorize incidents based on the type of incident and event, as shown in table 5.

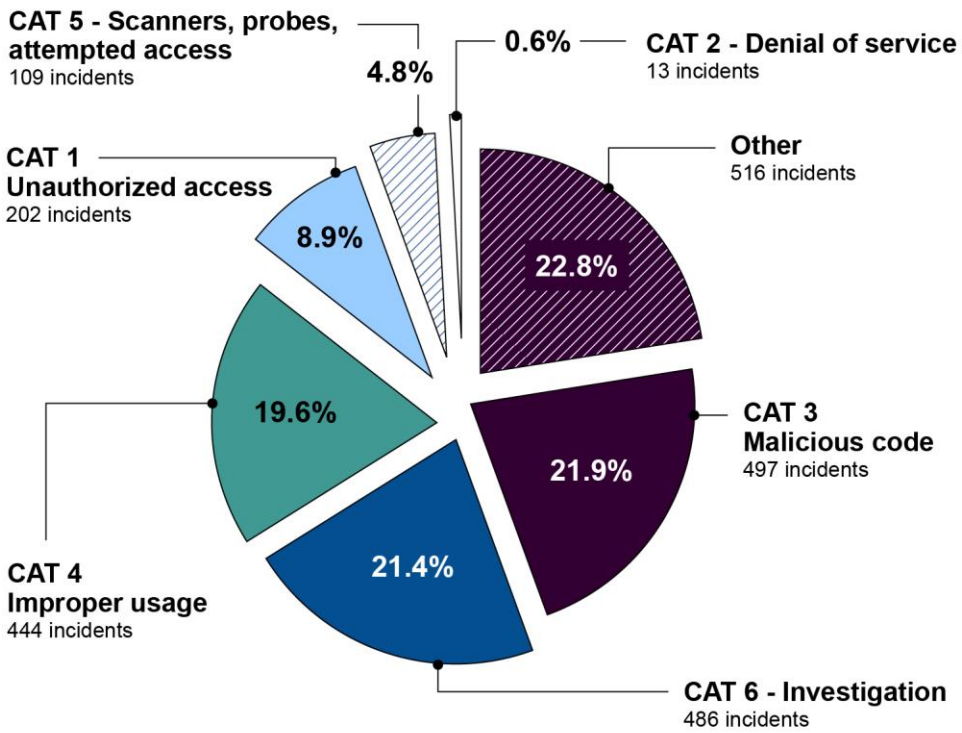
Table 5: US-CERT Incident Categories

Category	Name	Description
CAT 1	Unauthorized access	In this category, an individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
CAT 2	Denial of service	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the denial-of-service attack.
CAT 3	Malicious code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.
CAT 4	Improper usage	A person violates acceptable computing use policies.
CAT 5	Scans, probes, and attempted access	This category includes any activity that seeks to access or identify a federal agency's computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Source: List of cyber threat attack vectors developed by US-CERT and made available on their website. I GAO-16-501.

As shown in figure 9, the 11 agencies reported incidents affecting high-impact systems in each of the six incident categories. For example, 8 of the 11 agencies that responded reported malicious code incidents, accounting for about 22 percent of the total. In addition, improper usage accounted for about 20 percent of the total, occurring across 7 agencies. Further, one agency reported incidents involving the loss of data as "other."[13]

Figure 9: Incidents Affecting High-Impact Systems During Fiscal Year 2014, as Reported by 11 Agencies



Source: GAO summary based on responses to GAO survey. | GAO-16-501

[13]One agency's response accounted for all of the incidents categorized as "other." According to this agency, it used an additional category, "loss of data."

Half of the agencies with one or more high-impact system provided examples of significant incidents affecting their systems. Examples included incidents involving contractors using remote access, employees receiving and opening the attachments of phishing e-mails from spoofed addresses, and improper usage. The impact associated with these incidents included the agency disconnecting infected systems and the exposure and loss of personally identifiable information.

Various Government Entities Provide Guidance and Efforts Intended to Help Protect Systems

With the number of threats and incidents affecting the confidentiality, integrity, and availability of federal systems, government entities have provided guidance and established initiatives and services to aid agencies in protecting their systems, including those categorized as high impact. Agencies surveyed reported that available guidance was generally useful, and half of the reporting agencies indicated that they would like additional guidance. In addition, agencies reported that they are in the process of implementing various federal initiatives designed to help protect their high-impact systems.

Agencies Generally Found Available Guidance to be Useful

Agencies rely on different types of federal guidance to protect their high-impact systems; however, the agencies we surveyed reported that some guidance is more useful than other guidance. Guidance used to help protect high-impact systems includes, but is not limited to

- NIST publications,
- OMB memoranda,
- agency-specific guidance,
- Defense Information Systems Agency—security technical implementation guides,
- National Security Agency guidance, and
- Committee on National Security Systems guidance.

NIST publications—NIST provides various agency guidance, including standards and special publications (SP). Standards include those related to cryptography, system categorization, and minimum security requirements for federal systems. For example, as described earlier in this report, FIPS Pub 199 addresses requirements for categorizing systems as low, moderate, or high impact. In addition, NIST FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*, requires that agencies meet the minimum security

requirements by selecting the appropriate security controls and assurance requirements as described in NIST SP 800-53.[14]

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides a catalog of security and privacy controls for federal information systems and a process for selecting controls to protect organizational operations and assets. This publication provides baseline security controls for low-, moderate-, and high-impact systems, and agencies have the ability to tailor or supplement their security requirements and policies based on agency mission, business requirements, and operating environment. Baseline controls are the starting point for the security control selection process and are chosen based on the system's impact level as categorized by the agency. For example, there are 120 baseline controls for low-impact systems to be used as the starting point for the tailoring process. Controls for moderate-impact systems include not only the 120 baseline controls used for low-impact systems, but also an additional 124 baseline controls. For high-impact systems, there are 83 specific baseline controls that should be considered in addition to the baseline controls for low- and moderate-impact systems.

Security control topics covered by SP 800-53 include access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and service acquisition, system and communications protection, system and information integrity, and program management.

In addition to SP 800-53, agencies can use other special publications for identifying threats and reporting cybersecurity incidents, such as SP 800-37, *Guide for Applying the Risk Management Framework to Federal*

[14]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations,* SP 800-53, Revision 4 (Gaithersburg, MD: April 2013).

Information Systems,[15] and SP 800-61, *Computer Security Incident Handling*.[16] NIST also offers a host of other security and privacy guidelines, recommendations and reference materials, and reports of research findings.

OMB memoranda—OMB provides multiple forms of guidance on the management of federal information security resources, including memoranda such as (1) M-14-03, *Enhancing the Security of Federal Information and Information Systems*,[17] which provides agencies with direction for managing information security risk on a continuous basis, including the required security monitoring controls; (2) M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*,[18] which requires all publicly-accessible federal websites and web services to provide service through a secure connection, such as the Hypertext Transfer Protocol Secure web connection; and (3) M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*,[19] which addresses agency breach notification policy and reporting to US CERT. OMB also leads several government-wide initiatives, some of which are described later in this report, related to agencies' responsibilities in ensuring cybersecurity protections for federal information systems.

Further, FISMA requires that OMB amend or revise *Circular A-130*[20] to eliminate certain reporting no later than December 18, 2015 (one year after enactment, which was December 18, 2014). OMB has issued a

[15]National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* SP 800-37, Revision 1 (Gaithersburg, MD: February 2010).

[16]National Institute of Standards and Technology, *Computer Incident Handling Guide,* SP 800-61, Revision 2 (Gaithersburg, MD: August 2012).

[17]Office of Management and Budget, *M-14-03: Enhancing the Security of Federal Information and Information Systems* (Washington, D.C.: Nov. 18, 2013).

[18]Office of Management and Budget, *M-15-13: Policy to Require Secure Connections across Federal Websites and Web Services* (Washington, D.C.: June 8, 2015).

[19]Office of Management and Budget, *M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (Washington, D.C.: May 22, 2007).

[20]Office of management and Budget, *Circular Number A-130: Management of Federal Information Resources*, (Washington, D.C.: Nov. 28, 2000).

draft, but as of April 2016, OMB had not released the revised A-130. According to OMB staff, the office is in the process of reviewing and addressing agency comments received through early April; they will then need to put the guidance through OMB's internal clearance process before releasing it publicly. However, until such guidance is provided, agencies may continue to expend scarce resources on unnecessary reporting.

Agency-specific guidance—Federal agencies develop their own policies and procedures for the system controls that protect the information security needs of their computing systems, following the control structure outlined in SP 800-53. For example, SP 800-53 requirements may defer to organization-defined parameters, such as frequency of testing; agency-specific guidance will define these parameters.

Defense Information Systems Agency security technical implementation guides—The agency provides technical guidance for information systems and software that encompasses policy requirements for security programs and best practices for information assurance-enabled applications. According to the agency, the guides follow the baseline framework of NIST SP 800-53 security controls and cover various technical areas, including application security, mainframe, Windows, SQL server, Oracle databases, and network infrastructure.

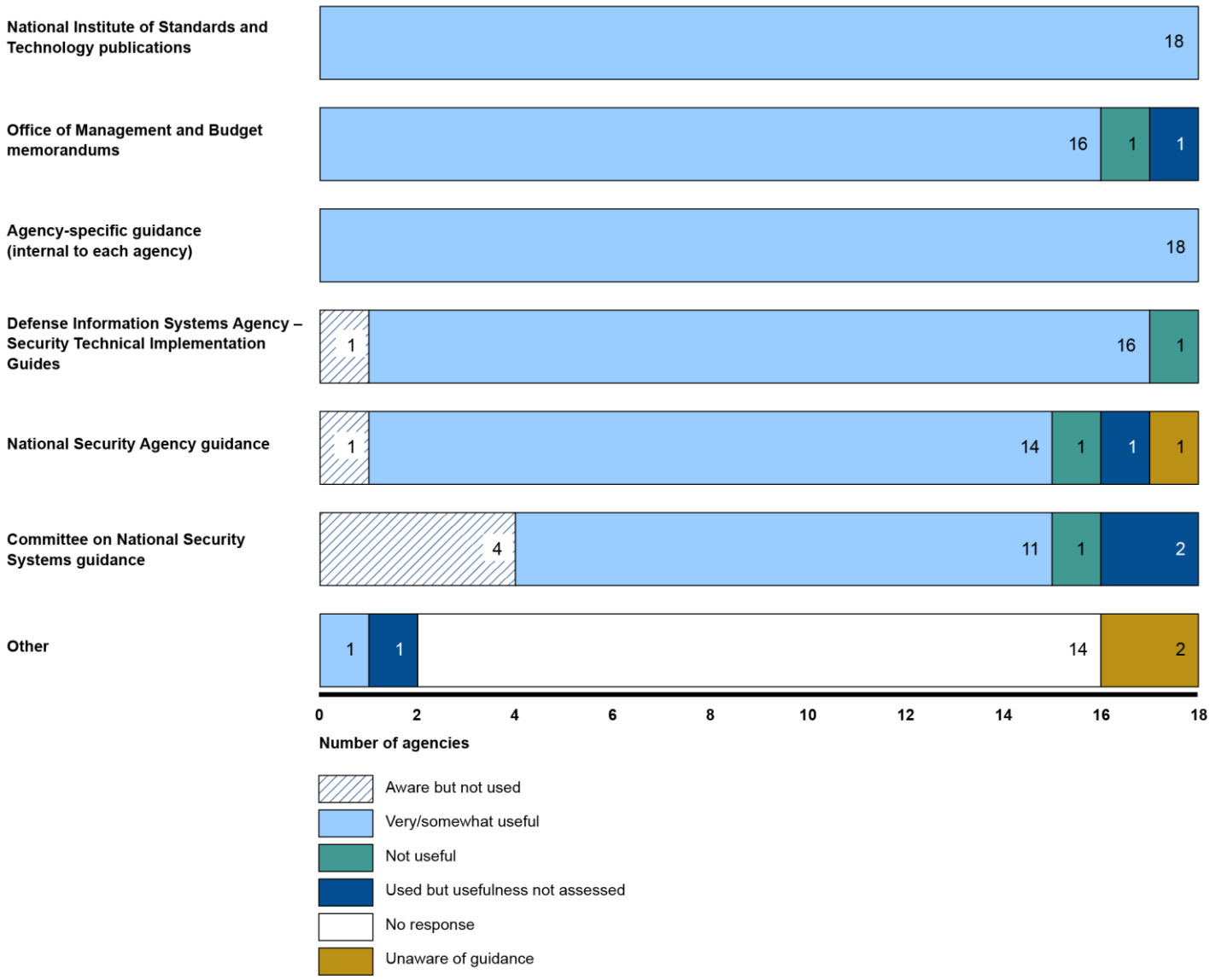
National Security Agency guidance—The agency develops and distributes configuration management guidance such as Oracle, Windows, and password policies to address security vulnerabilities.

Committee on National Security Systems guidance—This guidance sets national-level information assurance policies, directives, instruction, operational procedures, guidance, and advisories for national security systems. It provides a technical database for developing effective strategies and countermeasures for protecting national security systems. Policies related to protecting and securing high-impact systems include risk management, information sharing, incident response and vulnerability reporting, and controlled access protection. Such guidance may be used for systems that are not considered national security systems, such as high-impact systems.

In responding to our survey, the 18 agencies with high-impact systems reported that they found various types of guidance useful. As indicated in figure 10, most agencies reported that NIST and their own agency-

specific guidance were very or somewhat useful. Most also indicated that OMB and other guidance was very or somewhat useful.

Figure 10: Usefulness of Guidance to Agencies in Protection of High-Impact Systems, as Reported by 18 Agencies



Source: GAO summary based on responses to GAO survey. | GAO-16-501

Various Federal Initiatives Are Intended to Protect Systems, Including Those Considered High Impact

DHS and OMB have initiated various efforts intended to protect federal systems. These include, but are not limited to, DHS's May 2015 Binding Operational Directive,[21] OMB's 30-day Cybersecurity Sprint,[22] the October 2015 *Cybersecurity Strategy and Implementation Plan*,[23] and the recently issued President's *Cybersecurity National Action Plan*.[24]

FISMA gives statutory authority to DHS to issue binding operational directives to federal agencies regarding the specific actions that agencies need to take to address specific cyber threats and vulnerabilities. Implementation of these directives is compulsory for the agencies.

On May 21, 2015, DHS issued its first directive, which requires all departments and agencies to review and mitigate all critical vulnerabilities on their Internet-facing systems. DHS identifies the vulnerabilities using scanning tools and reports the results to agencies on a weekly basis. Agencies are required to mitigate the DHS-identified vulnerabilities within 30 days of the report, or provide a detailed justification to DHS outlining any barriers, planned steps for resolution, and a timeframe for mitigation. The weekly reports illustrate the vulnerabilities detected, identify the affected systems, and provide mitigation guidance. According to DHS, critical vulnerabilities are typically remotely exploitable; have a low complexity to execute; use default or no authentication; and impact confidentiality, integrity, and availability. By their very nature, critical vulnerabilities detected through scanning are exposed to anyone with an Internet connection, are at imminent risk of exploitation by a malicious third party, and should be immediately addressed.

[21]Department of Homeland Security, *Binding Operational Directive BOD-15-01: Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems* (Washington, D.C.: May 21, 2015).

[22]Office of Management and Budget, Executive Office of the President; *Fact Sheet: Enhancing and Strengthening the Federal Government's Cybersecurity* (Washington, D.C.: June 12, 2015).

[23]Office of Management and Budget, *M-16-04: Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (Washington, D.C.: Oct. 30, 2015).

[24]The White House, Office of the Press Secretary, *Fact Sheet: Cybersecurity National Action Plan* (Washington, D.C.: Feb. 9, 2016).

In addition, to improve the resilience of federal networks, in June 2015, OMB and the Federal Chief Information Officer directed agencies to review their cybersecurity policies, procedures, and practices, in what was called the 30-day Cybersecurity Sprint. The Cybersecurity Sprint instructed agencies to implement a number of immediate high-priority actions to enhance the cybersecurity of federal information and assets. They included

- deploying indicators provided by DHS regarding priority threat-actor techniques, tactics, and procedures to scan systems and check logs;
- patching critical vulnerabilities without delay;
- tightening policies and practices for privileged users; and
- accelerating implementation of multi-factor authentication for privileged users.

The *Cybersecurity Strategy and Implementation Plan*, issued in October 2015 was the result of the review of the federal government's cybersecurity policies, procedures, and practices addressed by the 30-day Cybersecurity Sprint Team. The goal of the 30-day Cybersecurity Sprint was to identify and address critical cybersecurity gaps and emerging priorities, and to make specific recommendations to address those gaps and priorities. The *Cybersecurity Strategy and Implementation Plan* addresses this goal by strengthening federal civilian cybersecurity through the following five objectives:

- identifying and protecting high value information and assets;
- detecting and responding to cyber incidents in a timely manner;
- recovering rapidly from incidents when they occur and accelerating the adoption of lessons learned from the Sprint assessment;
- recruiting and retaining a highly-qualified cybersecurity workforce; and
- acquiring and deploying existing and emerging technology efficiently.

OMB has not met key deadlines for issuing new plans and policies. The cybersecurity strategy specifies that OMB would (1) release a plan for implementing new cybersecurity shared services and (2) provide agencies with best practices and use cases for federal security operations centers by January 30, 2016. However, as of April 13, 2016, OMB had not released its plan for shared services and best practices for federal security operations centers. OMB staff stated that these initiatives are in progress and the office is actively collaborating with agencies to complete

these activities, but has not yet completed the plans and practices. Until OMB issues these plans and practices, agencies will not have the benefit of the efficiency associated with these services and practices to better protect their computing environments.

The strategy also addresses various initiatives, described in more detail later in this report, that are underway. According to the strategy and implementation plan:

- Continuous Diagnostics and Mitigation (CDM) addresses parts of each of the five stated objectives, and will help agencies develop a better understanding of the risks to their systems and networks through the improved identification and detection of cyber threats.
- Use of Personal Identity Verification (PIV) credentials for authenticating users' identity, particularly privileged users, should reduce the risk of identity fraud, tampering, counterfeiting, and exploitation.
- Agencies also are to rely on protections deployed through their Trusted Internet Connections (TIC), as publicly facing Internet connections are reduced and consolidated.
- In addition, agencies are to rely on the National Cybersecurity Protection System (NCPS, also known as EINSTEIN) for perimeter protection with threat-detection capabilities.

Further, in February 2016, the Administration announced the implementation of the *Cybersecurity National Action Plan*. This plan directs the federal government to take new action towards enhancing cybersecurity awareness and protections, and calls for long-term improvements in the approach to combating persistent threats and vulnerabilities across the federal government. The plan builds on the foundation laid by the *Cybersecurity Strategy and Implementation Plan*, including actions related to identifying and prioritizing highest value and most at-risk information technology assets, increasing the availability of government-wide shared cybersecurity services, expanding EINSTEIN and CDM programs, and recruiting cybersecurity talent.

In addition, the *Cybersecurity National Action Plan* highlights several proposed actions, such as the establishment of the Commission on Enhancing National Cybersecurity. The plan proposes that the commission be comprised of top strategic, business, and technical thinkers outside the government. This group will be tasked with making detailed recommendations on actions to take over the next decade to

enhance cybersecurity awareness and protections. Other actions cited in the plan include the modernization of government information technology to transform how the government manages cybersecurity through a proposed $3.1 billion Information Technology Modernization Fund, and the investment of more than $19 billion—according to the plan, a more than 35 percent increase over the 2016 enacted level—for cybersecurity as part of the President's fiscal year 2017 budget.

Agencies Have Initiatives Underway, but Implementation Varies

Various federal initiatives are under way that are intended to help protect agency systems, including those considered to be high impact. These initiatives, among others, include:

- CDM,
- PIV,
- TIC, and
- NCPS.

Continuous Diagnostics and Mitigation (CDM) program—Since fiscal year 2013, DHS has provided agencies the opportunity to use a suite of tools and capabilities to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These tools include sensors that perform automated searches for known cyber vulnerabilities, the results of which feed into dashboards that alert network managers, enabling agencies to allocate resources based on the risk. DHS also provides a federal dashboard-related infrastructure. The tools and services delivered through the CDM program are to provide the ability to enhance and automate existing agency continuous network monitoring capabilities, correlate and analyze critical security-related information, and enhance risk-based decision making at agency and federal levels.

OMB directed[25] agencies to develop and implement an agency-wide information security continuous monitoring strategy in accordance with

[25]M-14-03.

NIST guidance.[26] According to NIST, such a strategy should include defining key security metrics and establishing monitoring frequencies. Further, DHS, in partnership with the General Services Administration, established a government-wide acquisition vehicle for CDM that agencies must use if they require additional products/tools to leverage CDM services. There are three phases of CDM implementation:

- **Phase 1**: This phase involves deploying products to automate hardware and software asset management, configuration settings, and common vulnerability management capabilities. According to the *Cybersecurity Strategy and Implementation Plan*, DHS purchased phase 1 tools and integration services for all participating agencies in fiscal year 2015, and implementation will result in coverage for all of the agencies in our review.
- **Phase 2:** This phase intends to address privilege management and infrastructure integrity by allowing agencies to monitor users on their networks and to detect whether users are engaging in unauthorized activity. According to the *Cybersecurity Strategy and Implementation Plan*, DHS is to provide agencies with additional Phase 2 capabilities throughout fiscal year 2016, with the full suite of CDM phase 2 capabilities delivered by the end of the fiscal year. The strategy notes that such capabilities are intended to ensure that all employees and contractors at participating agencies are using appropriately secure methods to access federal systems.
- **Phase 3**: According to DHS, this phase is intended to address boundary protection and event management for managing the security life cycle. It focuses on detecting unusual activity inside agency networks and alerting security personnel. The agency plans to provide 97 percent of federal agencies the services they need for CDM phase 3 in fiscal year 2017.

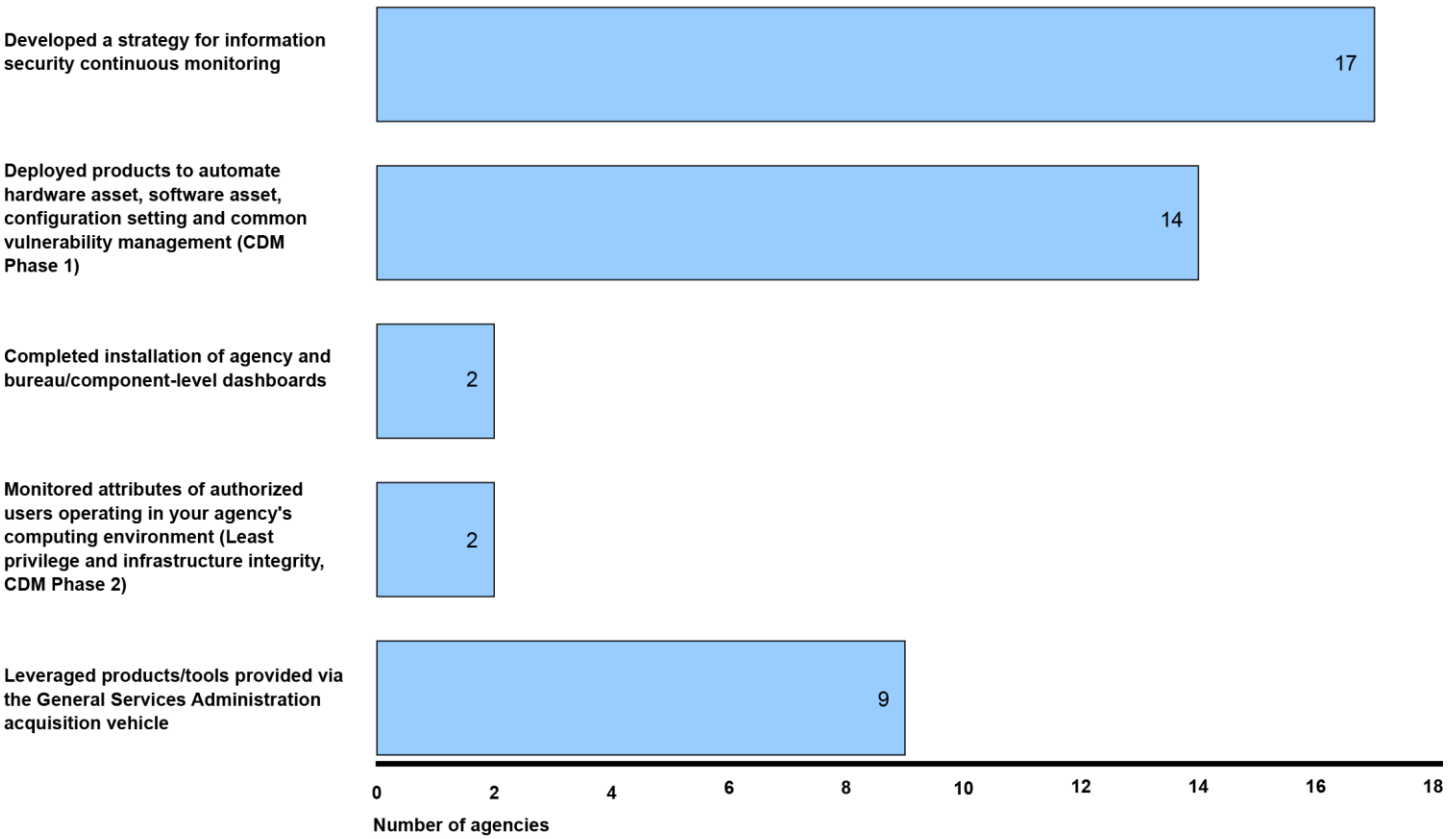
As shown in figure 11, most agencies are in the early stages of CDM implementation. Seventeen[27] of the agencies surveyed indicated they

[26]National Institute of Standards and Technology, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, SP 800-137 (Gaithersburg, MD: Sept. 2011).

[27]The Department of Defense, one of the 18 agencies with high-impact systems, is not required to participate in the Continuous Diagnostic and Mitigation program.

have developed a strategy for information security continuous monitoring. Additionally, according to survey responses, 14 of the 17 have deployed products to automate hardware and software asset configuration settings and common vulnerability management. Further, more than half of the agencies noted they had leveraged products/tools provided through General Services Administration's acquisition vehicle. However, only 2 of the 17 agencies reported that they had completed installation of agency and bureau/component-level dashboards, and monitored attributes of authorized users operating in their agency's computing environment.

Figure 11: Agency Implementation of Government-wide Initiatives Related to the Continuous Diagnostics and Mitigation Programs, as Reported by 17[a] Agencies with High-Impact Systems



Source: GAO summary based on responses to GAO survey. | GAO-16-501

[a]The Department of Defense, one of the 18 agencies with high-impact systems, is not required to participate in the Continuous Diagnostic and Mitigation program.

Personal Identity Verification—PIV has been a mandated federal standard[28] since August 2004, and is intended to increase the use of federal smartcard credentials, such as personal identity verification and common access cards that provide multifactor authentication, digital signature, and encryption capabilities for agency employees and contractors. Strong authentication can provide a higher level of assurance when authorizing users' access to federal information systems. PIV includes authentication measures for both privileged and unprivileged users.[29] Issued in the form of an access card, PIV may be used to authenticate the identity of the cardholder in a physical access control environment (e.g. a federal facility with physical entry doors with guards at checkpoints), or may be used to authenticate the cardholder in support of decisions concerning logical access to information resources (e.g., a cardholder may log into the agency network using the PIV card). The Cybersecurity Sprint directed agencies to immediately implement PIV for 100 percent of their privileged users and for 75 percent of non-privileged users.

In September 2011, we reported that a lack of prioritization had kept agencies from being able to require the use of PIV credentials for logical system access.[30] We made recommendations to nine agencies, including OMB, regarding achieving greater implementation of PIV capabilities. Seven of the nine agencies agreed with our recommendations or discussed actions they were taking to address them; two agencies did not comment. To date, at least 18 of the 24 recommendations have been implemented.

In July 2015, the Federal Chief Information Officer reported the results of the Cybersecurity Sprint, which are shown in table 6. Four agencies met the goal for privileged users and 13 met the goal for non-privileged users.

[28]Department of Homeland Security, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors* (Washington, D.C.: Aug. 27, 2004).

[29]Privileged users have extended network access user accounts with elevated privileges, and unprivileged users do not.

[30]GAO, *Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Card*, GAO-11-751 (Washington, D.C.: Sept. 20, 2011).

Table 6: July 2015 Cybersecurity Sprint Results for Personal Identity Verification Implementation for 18 Agencies that Had High-Impact Systems

	Number of agencies	
Percent implemented	**For privileged users**	**For unprivileged users**
100	4	0
90 – 99	6	4
75 – 89	3	9
50 – 74	3	1
25 – 49	0	3
0 – 24	2	1

Source: GAO analysis of agency data. I GAO-16-501 .

Trusted Internet Connection—In November 2007, OMB began this initiative to secure federal agencies' external network connections, including Internet connections, and improve the government's incident response capability by reducing the number of agencies' external network connections and implementing security controls over the connections that remained.[31] In implementing TIC, agencies can either provide their own access points by becoming an access provider or seek service from these providers or an approved vendor. To obtain TIC services, some agencies rely on Networx, a program managed by the General Services Administration that serves as an acquisition vehicle for agencies to procure telecommunication, network, wireless, and information technology security services, including TIC services, from among multiple vendors. Additionally, DHS, in collaboration with the General Services Administration's Federal Risk Authorization Management Program, updated TIC architecture requirements to give agencies the opportunity to access their own cloud services through a TIC-compliant agency network, or work with another agency designated as a TIC access provider and leverage their external connection's perimeter security.

[31]Office of Management and Budget, *M-08-05: Implementation of Trusted Internet Connections* (Washington, D.C.: Nov. 20, 2007).

In 2010, we reported that none of the agencies had met the requirements of the TIC initiative.[32] However, although most agencies had experienced delays in implementation, most had made progress towards reducing their external network connections. Further, through these efforts, agencies had experienced benefits such as improved security and network management.

In response to our survey, 17 agencies[33] with high-impact systems that were required to implement TIC reported that at least 80 percent of their TIC access points are using external connections to their networks. Seven of these agencies indicated that 100 percent of their TIC access points are using external connections for access to their network, 7 others are using 90 percent or more, and the 3 other agencies are using 80 percent or more. In addition, most surveyed agencies with high-impact systems either provided their own TIC services, or used the services provided by another agency. Additionally, 8 of the 17 agencies indicated the use of services offered via Networx.

National Cybersecurity Protection System—NCPS is an integrated system-of-systems that is intended to deliver a range of capabilities, including intrusion detection, intrusion prevention, analytics, and information sharing. The NCPS capabilities, operationally known as the EINSTEIN program, are one of a number of tools and capabilities that assist in federal network defense. Originally created in 2003, NCPS is intended to aid DHS in reducing and preventing computer network vulnerabilities across the federal government. Its analysts examine raw and summarized data from a wide variety of information sources to make determinations about potential attacks across the network traffic of participating federal agencies.

NCPS is intended to build successive layers of defense mechanisms into the federal government's information technology infrastructures. When NCPS intrusion detection sensors are deployed at a TIC location, the system monitors inbound and outbound network traffic, with the goal of allowing US-CERT, using NCPS and its supporting processes, to monitor

[32]GAO, *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies*, GAO-10-237 (Washington, D.C.: Mar 12, 2010).

[33]One agency did not respond to the question.

all traffic passing between the federal civilian network sensors and the Internet for malicious activity.

For the surveyed agencies, 15 of the 17 agencies[34] reported that traffic to/from their high-impact systems was routed through the NCPS sensors, while 2 of the 17 indicated that, although they use NCPS, traffic to/from their high-impact systems was not routed through the sensors.

In January 2016, we reported several issues related to the development and execution of NCPS. Specifically, NCPS compares network traffic to known patterns of malicious data, or "signatures," but does not detect deviations from predefined baselines of normal network behavior; does not monitor several types of network traffic; its "signatures" do not address threats that exploit many common security vulnerabilities; and it does not address malicious content within Web traffic.[35] We recommended, among other things, that DHS determine the feasibility of enhancing NCPS's current intrusion detection approach to include functionality that would detect deviations from normal network behavior baselines; the feasibility of developing enhancements to current intrusion detection capabilities to facilitate the scanning of traffic not currently scanned by NCPS; and for US-CERT to update the tool it uses to manage and deploy intrusion detection signatures to include the ability to more clearly link signatures to publicly available, open-source data repositories. DHS concurred with our recommendations and indicated it was taking action to implement them.

Services Are Available to Help Protect Systems, but Are Not Always Used

Various services are available that could help agencies protect their high-impact systems. As described in table 7, such services include, but are not limited to the

- Information Security and Identity Management Committee forums for agency collaboration,

[34]The Department of Defense, one of the 18 agencies with high-impact systems, indicated in the survey that their Internet defenses are the model for all versions of NCPS, and subsequently, all DOD traffic bound to/from the network goes through comprehensive defenses, but not the NCPS.

[35]GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: January 2016).

- US-CERT monthly operational bulletins,
- CyberStat reviews,
- National Cyber Investigative Joint Task Force information sharing,
- Federal Cybersecurity Coordination, Assessment, and Response Protocol shared situational awareness and coordinated incident response, and
- DHS Red and Blue Team exercises.

Our survey results indicated that participation levels varied for these services and some agencies found them more useful than others.

Table 7: Services Available for Federal Agencies to Protect Their High-Impact Information Systems

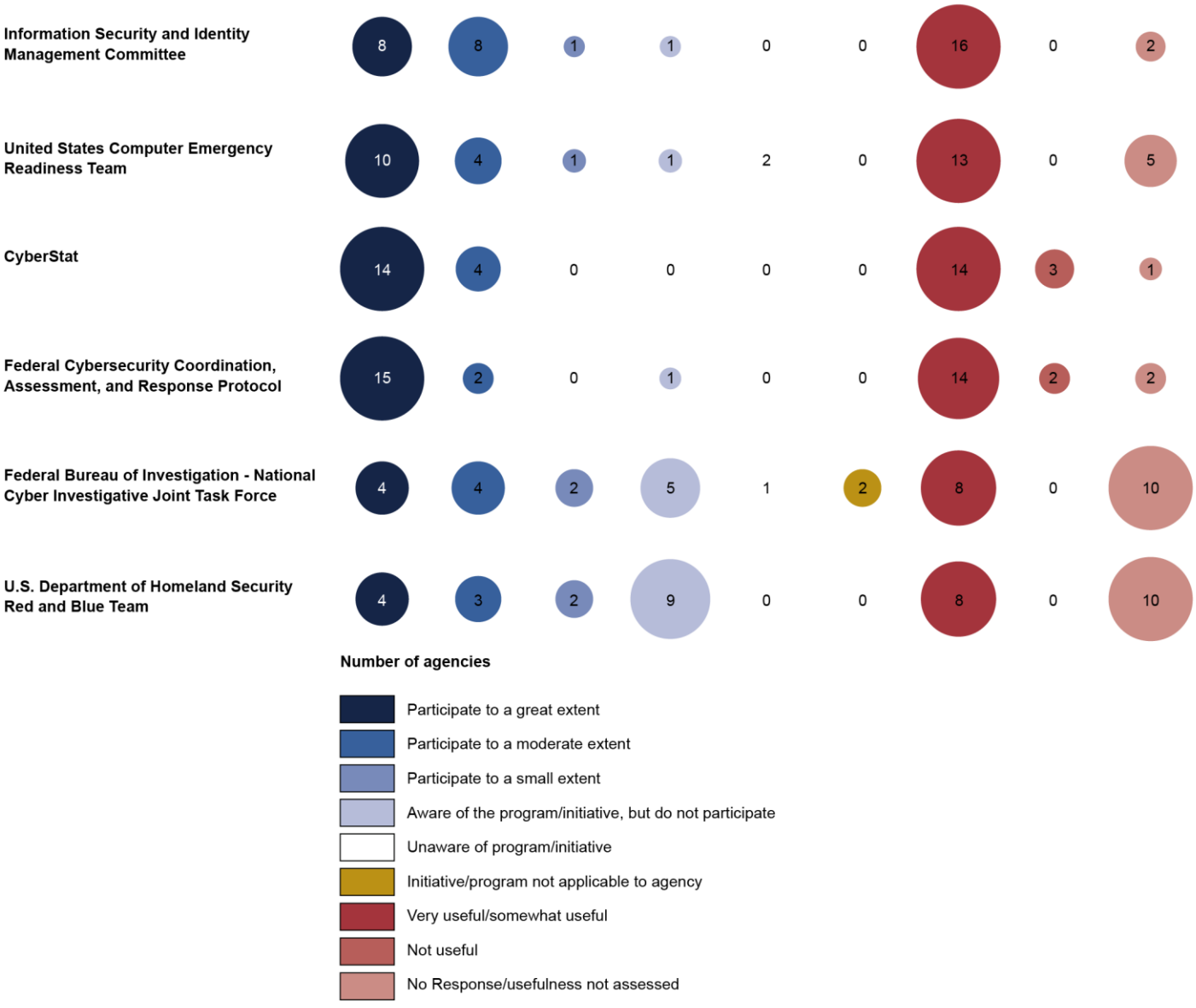
Service	Description
Information Security and Identity Management Committee	Intended to provide a consensus-based forum to support the Federal CIO Council. It enables chief information officers and chief information security officers to collaborate on identifying high-priority security and identity management initiatives.
US-CERT monthly operational bulletins	Intended to provide senior federal government information security officials and staff with actionable information to improve their organization's cybersecurity posture based on incidents observed, reported, or acted on by DHS and US-CERT.
CyberStat reviews	In-depth sessions with National Security Staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and discuss opportunities for collaboration. According to OMB, these interviews are face-to-face, evidence-based meetings intended to ensure agencies are accountable for their cybersecurity posture. The sessions are to assist the agency in developing focused strategies for improving their information security posture in areas where there are challenges.
National Cyber Investigative Joint Task Force	Organized by the Federal Bureau of Investigation in 2008, the task force is intended to be the focal point for all government agencies to coordinate, integrate, and share information related to domestic cyber threat investigations. The sharing of information provides connectivity to federal cyber centers and government agencies in the event of a cyber-intrusion 24/7.
Federal Cybersecurity Coordination, Assessment, and Response Protocol	Established in January 2012 to facilitate cybersecurity communication between agency chief information officers and chief information security officers responding to significant cyber incidents affecting federal information systems. The protocol is intended to provide the federal government with a rapidly implementable mechanism that will ensure shared situational awareness and coordinated response to imminent or on-going significant cyber incidents. According to OMB, existing processes and procedures for steady state information sharing and response between agencies continue to be used and operate in synchronization with the protocol.
DHS Red and Blue Team exercises	Intended to provide services to agencies for testing their systems with regard to potential attacks. A Red Team emulates a potential adversary's attack or exploitation capabilities against an agency's cybersecurity posture. The Blue Team defends an agency's information systems when the Red Team attacks, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group.

Source: GAO analysis of various government services. I GAO-16-501.

Although participation varied among the agencies we surveyed, most of those that chose to participate generally found the services to be effective resources to aid cybersecurity protection within their high-impact systems, as indicated in figure 12. Specifically,

- Eight of the 18 agencies reported that they greatly participated in the Information Security and Identity Management Committee forums, and most found the service very or somewhat useful.
- Ten of 18 agencies greatly participated with the US-CERT monthly operational bulletins, and most found the service very or somewhat useful.
- Fourteen of 18 agencies greatly participated with CyberStat reviews, and most found the service very or somewhat useful.
- Fifteen of 18 greatly participated with the federal Cybersecurity Coordination, Assessment, and Response Protocol, and most found the service very or somewhat useful.

Figure 12: Extent to Which Agencies Participated in and Found the Services to Protect Their High-Impact Systems Useful, as Reported by 18 Agencies



Source: GAO summary based on responses to GAO survey. | GAO-16-501

Although Federal Guidance, Initiatives, and Services Exist, Agencies Want Additional Help to Protect Their High-Impact Systems

Although the agencies surveyed reported that available guidance was generally useful, half of the agencies wanted more guidance. However, most of these agencies (nine) did not list any specific needs. A few offered suggestions, such as receiving guidance-setting priorities for current initiatives and increased OMB/DHS support for centralized enterprise services.

Also in our survey, half of the agencies reported that they wanted an expansion of federal initiatives and services to help protect their high-impact systems. For example, agencies noted that expediting CDM phases/implementation, sharing threat intelligence information, sharing attack vectors, and federal procurement activities leveraging shared services could be of benefit to them in further protecting their high-impact systems.

The *Cybersecurity Strategy and Implementation Plan* issued in October 2015 recognizes the need to address these concerns. For example, it notes that DHS will accelerate the deployment of CDM and EINSTEIN capabilities to all participating federal agencies to enhance detection of cyber vulnerabilities and protection from cyber threats. Further, the *Cybersecurity Act of 2015*,[36] enacted in December 2015, requires DHS to develop a capability to (1) accept cyber threat indicators and defensive measures from any non-federal entity in real time and (2) ensure that appropriate federal entities receive the shared indicators in an automated real-time manner.

[36]The *Cybersecurity Act of 2015* was enacted into law as Division N of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113 (Dec. 18, 2015).

Selected Agencies We Reviewed Did Not Always Implement Controls for Selected Systems Effectively

NASA, NRC, OPM, and VA had implemented numerous controls, such as completion of risk assessments, over selected systems. However, they had not always effectively implemented access controls, patch management, and contingency planning to protect the confidentiality, integrity and availability of these high-impact systems.[37] These weaknesses existed in part because the agencies had not effectively implemented elements of their information security programs. As a result, increased risk exists that sensitive information could be disclosed or modified without authorization, and system operations may be disrupted.

Access Controls Were Not Always Effectively Implemented

A basic management objective for any agency is to protect the resources that support its critical operations from unauthorized access. Agencies accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Access controls include those related to protecting system boundaries, identifying and authenticating users, authorizing access needed to perform job duties, encrypting sensitive data, and auditing and monitoring system activities. NIST and agency policies describe various specific controls to address each of these areas.

- **Boundary protection** controls pertain to the protection of a logical boundary around a system by implementing measures to prevent unauthorized information exchange across the boundary in either direction. Implementing multiple layers of security to protect an information system's boundaries can reduce the risk of a successful cyber attack.
- **Identification and authentication**—such as user account-password combinations—provides the basis for establishing accountability and for controlling access to systems.
- **Authorization** is based on the concept of "least privilege," which means that users should be granted the least amount of privileges necessary to perform their duties.

[37]These weaknesses are summarized here. However, due to the sensitive nature of the identified weaknesses, more detailed examples and any associated recommendations will be provided to each agency separately in limited distribution reports.

- **Cryptography** controls can be used to identify and authenticate users and help protect the integrity and confidentiality of data and computer programs by rendering data unintelligible to unauthorized users and by protecting the integrity of transmitted or stored data.
- **Audit and monitoring** involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity.

The four agencies implemented elements of these controls in the eight systems reviewed. However, as indicated in table 8, each of the systems had weaknesses in access controls, with almost all of the systems having weaknesses in all, or most, of the control areas. Specific examples of control weaknesses included administrators sharing accounts for authenticating to servers supporting five of the eight systems, rather than using unique accounts for accountability, and five of eight systems not being configured to log all key security events to identify inappropriate or unusual activity.[38]

Table 8: Access Control Weaknesses Identified for Eight Selected Systems

	NASA		NRC		OPM		VA	
	System 1	System 2	System 3	System 4	System 5	System 6	System 7	System 8
Boundary protection	X	X	X	X	X	X	X	X
Identification and authentication	X	X	X	X	X	X	X	
Authorization	X	X	X	X	X	X	X	X
Cryptography	X		X			X		
Audit and monitoring	X		X	X	X	X	X	X

Source: GAO testing of controls for selected systems at selected agencies. I GAO-16-501.

Note: X – one or more control weaknesses identified.

Unless access controls are effectively implemented, data maintained on selected systems will be at increased risk of unauthorized access, modification, and disclosure, possibly without being detected.

[38]Due to the sensitive nature of the identified weaknesses, more detailed examples and any associated recommendations will be provided to each agency separately in limited distribution reports.

Up-to-date Patches Were Not Always Installed to Support Selected Systems

Patch management is an important element in mitigating the risks associated with known vulnerabilities. When vulnerabilities are discovered, the vendor may release an update to mitigate the risk. If the update is not applied in a timely manner, an attacker may exploit a vulnerability not yet mitigated, enabling unauthorized access to information systems or enabling users to have access to greater privileges than authorized. NIST recommends security-related software updates, such as patches, to be installed within an organization-defined time period of the release of the update. At the four selected agencies, the required time period for installing critical patches ranged from 7 to 30 days.

However, for six systems we reviewed where patches were available, agencies had not installed certain patches in a timely manner. For example, for one system at one agency, 34 critical patches were missing for the three servers and four workstations tested. One of the missing server patches was initially released in May 2012, and one of the missing workstation patches (occurring on 3 of the 4 servers) was released in April 2011. By not installing patches in a timely manner, agencies are at increased risk that known vulnerabilities in their systems may be exploited.[39]

Selected Agencies Had Contingency Plans in Place for Systems Reviewed, but Not All Plans Were Comprehensive and Appropriate Tests Were Not Always Conducted

Federal law and guidance emphasize the importance of agencies having effective contingency planning for interruptions in service, which is especially important when high-impact systems are involved. FISMA requires that each agency document plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. In addition, according to NIST, effective contingency planning includes, among other things, development of contingency planning policies and procedures, and a contingency plan that includes the following ten elements, with the last two being specifically for high-impact systems:

1. A review and approval of the plan by agency-defined personnel.

[39]Due to the sensitive nature of the identified weaknesses, more detailed examples and any associated recommendations will be provided to each agency separately in limited distribution reports.

2. Coordination of contingency planning with incident handling activities.
3. Updating plans according to an agency-defined frequency to address changes to the agency, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
4. Identification of essential mission and business functions and their associated contingency requirements.
5. Recovery objectives, restoration priorities, and metrics.
6. Contingency roles, responsibilities, and assigned individuals with contact information.
7. How essential mission and business functions will be maintained despite an information system disruption, compromise, or failure.
8. How the full information system will be restored without deterioration of the security safeguards.
9. (For a high-impact system): How essential mission and business functions will be resumed within an organization-defined time period.
10. (For a high-impact system): How capacity planning will be conducted so that necessary capacity for information processing, telecommunications, and environmental support will be maintained during contingency operations.

In addition, NIST recommends that agencies test the contingency plan for information systems according to an agency-defined frequency using defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan. Further, for high-impact systems, NIST recommends that the agency test its contingency plans at a designated alternate processing site. An alternate processing site provides processing capability in the event that the primary processing site is not available.

For the selected systems, agencies had included various elements in their contingency plans, such as identifying mission and business functions, roles and responsibilities, and full system restoration. However, they did not always include other elements in their contingency plan, as shown in table 9.

Table 9: Agency Compliance with Contingency Plan Elements

Element	NASA		NRC		OPM		VA	
	System 1	System 2	System 3	System 4	System 5	System 6	System 7	System 8
Review and approve	●	●	●	◐	◐	◐	●	●
Coordination of contingency planning with incident handling activities	●	●	●	●	○	○	◐	◐
Update plan to address changes	●	●	●	●	●	●	●	●
Identify mission and business functions	●	●	●	●	●	●	●	●
Define recovery objectives, restoration priorities, and metrics	●	●	●	●	●	●	●	●
Contingency roles, responsibilities, and contact information	●	●	●	●	●	●	●	●
Address maintenance of essential missions and business functions	●	●	●	●	●	●	●	●
Address full information system restoration	●	●	●	●	●	●	●	●
Plan for resumption of essential mission and business functions within an organization-defined time period	●	◐	◐	◐	●	◐	●	●
Conduct capacity planning	●	●	●	●	●	●	●	●

Source: GAO analysis of agency data. I GAO-16-501.

Note: ● — generally met; ◐— partially met; ○ — not met

In addition, not all plans had been appropriately tested as required for a high-impact system. Specifically,

- NASA— According to NASA's 2011 *IT Security Handbook on Contingency Planning*, the organization-defined frequency for contingency plan tests is annually for high-impact systems. The handbook also states that an alternate site test should occur every three years for high-impact systems. NASA had tested one of its plans within the agency's required time frame at the alternate processing site. However, although NASA had tested another plan annually, the agency did not test the plan at the alternate processing site. NASA explained it did not test the plan at an alternate site since the real-time operational nature of the system does not allow for the interruption of services to perform contingency exercises; however, the agency stated it uses tabletop exercises and test bed environments to exercise the plan.

- NRC— According to NRC's July 2015 *Computer Security Standard*, an unclassified control provider shall test the plan for the information system at least annually and at least every three years at the alternate processing site. For one system's plan, NRC had conducted a functional test in 2014 and a component test in 2015, but the agency did not test the plan at the alternate processing site in 2014 or 2015. However, the latest test of the plan at the alternate processing site was March 2011. For another plan, NRC had conducted two table-top exercises and one component test in 2014, and had tested the system plan at the alternate processing site in 2015.
- OPM— According to OPM's 2011 *Information Security Privacy Policy Handbook*, system owners shall ensure the contingency plan for the information system is tested and/or executed at least annually. In addition, system owners shall ensure testing of the contingency plan at the alternate processing site. OPM had conducted table-top exercises for one of its plans annually, and another plan had been tested in 2014, but for 2015, instead relied on disaster recovery testing for this system's operating environment. This disaster recovery test occurred at an alternate processing site; however, OPM had not established an alternate site for its other system.
- VA—The agency's 2010 data center directive states that all VA emergency plans shall be tested at least once a year. In addition, VA's 2011 handbook on information system contingency planning states that contingency plans must be tested at an alternate site if established. VA had tested one of its plans annually through a table-top exercise and had performed a table-top exercise on another system's plan once in 2015 because the system was new. VA had not tested either of the plans at its alternate processing site.

Without including important information in its contingency plans for their high-impact systems and sufficiently testing its plans, agencies are at an increased risk of not being able to recover from a service disruption.[40]

[40]Due to the sensitive nature of the identified weaknesses, more detailed examples and any associated recommendations will be provided to each agency separately in limited distribution reports.

Selected Agencies Had Developed Security Programs, but Had Not Effectively Implemented Key Elements

A key reason for the information security weaknesses in selected systems at the four agencies was that, although the agencies have developed and documented comprehensive agency-wide information security programs, they had not effectively implemented elements of the programs.

An agency-wide information security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes the following components:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- plans for providing adequate information security for networks, facilities, and systems or group of information systems, as appropriate;
- training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems; and
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, or practices of the agency.

In addition, the current administration has made continuous monitoring of federal information systems a top cybersecurity priority. Continuous monitoring of security controls employed within or inherited by the system is an important aspect of managing risk to information from the operation and use of information systems.

Agencies developed risk assessments for selected systems

Identifying and assessing information security risks is essential to determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that the

policies and controls operate as intended. According to NIST,[41] risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. Each of the four selected agencies had policies in place for developing risk assessments in accordance with the elements described by NIST.

The four agencies we reviewed had developed a risk assessment for each of the selected systems. All of the assessments included the identification of threat sources and vulnerabilities, as well as a determination of likelihood of occurrence and magnitude of impact.

Although agencies had developed security plans, consideration of the security baseline controls for high-impact systems varied

An objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place or planned to meet those requirements. NIST describes the various elements that should be included in a security plan. These elements include:

- defining the authorization boundary for the system,
- describing the operational context of the information system (mission and business processes),
- describing the operational environment for the information system and relationships with or connections to other information systems, and
- providing an overview of the security requirements for the systems.

In addition, plans may cross reference other plans where common controls may be implemented (e.g. a system may rely on controls from another system). Further, the plan should describe the security controls in place or planned for meeting security requirements, including a rationale for tailoring and supplementation decisions. These controls, as described earlier in this report, are chosen based on the system categorization of

[41]See National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, SP 800-30, Rev 1 (Gaithersburg, MD: September 2012), and NIST SP 800-53.

low, moderate, or high impact. There are 83 controls specific to the baseline for high-impact systems. An agency initiates the tailoring process to modify and align the controls more closely with the specific conditions within the agency.

Agencies had developed security plans for each of the eight selected systems; the plans included authorization boundaries, operational context and environment, and security requirements. However, at OPM, one system's plan referred to controls provided by another system, but the other system's plan did not address these controls.

Further, the extent to which the eight plans addressed controls specific to high-impact systems varied widely, as shown in table 10. Plans for both NASA systems and one OPM system addressed all, or almost all, of the 83 controls; however, the others addressed fewer than 60 of the 83 controls, and one system at VA did not address any of the controls. Without comprehensive security plans that include controls appropriate and specific to high-impact systems, or explaining the rationale for not including them, systems will be at increased risk that the confidentiality, integrity, and availability of sensitive data and resources will not be adequately protected.

Table 10: Specific High-Impact Controls Addressed in Selected Systems' Security Plans

	NASA		NRC		OPM		VA	
	System 1	System 2	System 3	System 4	System 5	System 6	System 7	System 8
Addressed in plan (including rationale if not implemented)	80	83	55	52	40	82	0	12
Not addressed (including no rationale for exclusion)	3	0	28	31	43	1	83	71

Source: GAO analysis of security plans for selected systems. I GAO-16-501.

Agencies did not always ensure individuals with significant security responsibilities received specialized training

Role-based training helps ensure that individuals with significant security responsibilities carry out their job in a manner that protects the systems they work with as part of their job duties. NIST recommends that agencies establish training policies and procedures to facilitate the implementation of the training policies and provide specialized security training of individuals assigned security roles and responsibilities.

The four agencies we reviewed had all established policy and procedural requirements for individuals with significant IT security responsibilities, and had established a tracking mechanism for monitoring whether

personnel had completed the training. In addition, all four agencies had established specialized IT security training policies through agency handbooks, plans, or other means.

However, agencies had shortcomings in monitoring whether training had been completed or not. We sampled 180 individuals[42] across the four agencies. The agencies were unable to provide us with active training records for 71 individuals, with reasons for this varying. For example, OPM noted that it did not centrally track training records for contractors of one of the systems we reviewed, and others in our sample did not meet their internal criteria for needing specialized training. In addition, NRC explained that they did not believe 16 of the individuals were in roles that required specialized training, noting that the agency was in the process of updating system security documentation associated with one of the selected systems, and at the time of our field work, the documentation we reviewed had not yet been updated. Agencies also reported that 8 individuals in our sample had separated from the respective agency.

Of 180 individuals we selected across the four agencies, we received 109 active training records from the agencies. From these training records, we found that 61 individuals had completed a form of specialized security training for fiscal year 2015. Agencies had various reasons why the remaining 48 individuals had not completed training. For example,

- NASA issued a role-based training handbook in May 2015. Agency officials explained that, until that time, the agency had not clearly defined role-based training requirements. At the time of our review, officials noted that, for the 25 individuals who had not completed training, it was likely that either an individual's role had not yet been defined, or they were still in the process of implementing the requirements specified in the handbook.
- NRC officials stated that 3 of the 27 individuals it tracked did not have fiscal year 2015 requirements assigned based on their role. In

[42]For each agency reviewed, we developed a list of employees and contractors with potentially significant security responsibilities for the high-impact systems we reviewed. We identified those individuals by (1) examining system security plans, contingency plans, incident response plans and (2) including system and database administrators we met with for system testing. We then selected a non-generalizable sample from each list, which resulted in a total sample of 180 individuals.

addition, NRC reported that 3 individuals did not complete all fiscal year 2015 role-based requirements.

- VA explained that it could not provide fiscal year 2015 specialized security training records for the remaining 17 individuals due to the individuals having completed requirements prior to 2015 or in fiscal year 2016. The agency demonstrated that 15 out of 17 individuals had completed specialized security training prior to fiscal year 2015, and 2 individuals had completed specialized security training in fiscal year 2016.

Table 11 summarizes the number of individuals at each of the agencies who had completed the specialized security training.

Table 11: Number of Individuals Who Completed Specialized Security Training for Fiscal Year 2015

Number of individuals	NASA	NRC	OPM	VA	Total
Completed specialized IT security training	11	21	15	14	**61**
Not completed	25	6	0	17	**48**
Total tracked for fiscal year 2015	**36**	**27**	**15**	**31**	**109**
Total not tracked for fiscal year 2015	**10**	**16**	**31**	**14**	**71**

Source: GAO analysis of agency training data. I GAO-16-501.

If agencies do not provide and monitor specialized training, they cannot ensure that personnel with significant security responsibilities have the appropriate information they need to protect their systems.

Most agencies had conducted information security control assessments for systems, but not all assessments were comprehensive

Another key element of an information security program is to test and evaluate policies, procedures, and controls to determine whether they are effective and operating as intended. These assessments are intended to identify vulnerabilities and compliance with agency policies and procedures. NIST recommends agencies do the following in completing their security control assessments:

- Develop a security assessment plan that describes the scope of the assessment, to include the security controls assessed, procedures used, and the assessment environment, team, and assessment roles and responsibilities.
- Assess the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the

desired outcome with respect to meeting established security requirements.

- Produce a security assessment report that documents the results of the assessment.
- Provide the results of the security control assessment to agency officials.
- Use assessors with an organization-defined level of independence for conducting control assessments.

As shown in table 12, three of the four agencies had conducted information security control assessments for selected systems; one had not. Specifically, one of the VA systems had not undergone an assessment since 2011, and its other system had never been through the assessment process. In addition, although NASA had assessment plans, the plans did not include the test procedures to be performed. Instead, its independent assessor maintained the procedures used for testing, and the agency did not review or approve them in advance to ensure that the procedures were comprehensive.

Table 12: Security Control Assessments for Selected Systems

	NASA		NRC		OPM		VA	
	System 1	System 2	System 3	System 4	System 5	System 6	System 7	System 8
Plan included scope, controls, procedures, and roles	◐	◐	◐	●	●	●	○	○
Assessed controls	●	●	●	◐	●	●	○	○
Produced report	●	●	●	●	●	●	○	○
Provided results to officials	●	●	●	●	●	●	○	○
Used independent assessor	●	●	●	●	●	●	○	○

Source: GAO analysis of control assessments of selected systems. | GAO-16-501

Note: ● – Met ◐ - Partially met ○ – Did not meet. According to agency officials, the last assessment for system 7 occurred prior to use of their new documentation system and they were unable to provide us with the assessment for review.

In addition, although the agencies had assessed security controls for six of the selected systems, their assessments were not comprehensive. For example, the agencies had not identified many of the weaknesses in access controls for these six systems that we identified during our examination of security controls as summarized earlier in this report.

If security assessment plans do not identify controls to be assessed or the procedures to be used, agency officials cannot be assured that controls are operating as intended. Further, without comprehensive assessments, agencies may not be aware of additional control weaknesses that could endanger the confidentiality, integrity, and availability of sensitive data.

Agencies had developed remedial action plans, but the plans did not include all the required elements

A remedial action plan is a key component of an agency's information security program, as described in FISMA. Such a plan assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. NIST recommends that agencies develop a plan of action and milestones (POA&M) for an information system to document the agency's planned remedial actions to correct identified weaknesses. NIST also states that a POA&M is subject to requirements established by OMB. According to OMB, the elements of a POA&M should include:

- specific vulnerability or weakness,
- office or organization responsible for resolving the weakness,
- estimated funding required to resolve the weakness,
- source of the funding required to resolve the weakness,
- scheduled completion date for resolving the weakness,
- key milestones with completion dates,
- changes to milestones and completion dates,
- source that identified the weakness, and
- status of the corrective action (ongoing, completed, etc.).

As shown in table 13, selected agencies had created a POA&M for the selected systems.[43] However, none of the plans included all of the required elements.

[43]One system did not have an active remedial action plan as noted in Table 13.

Table 13: Required Components for a Remedial Plan of Action and Milestones

	NASA		NRC		OPM		VA	
POA&M element	**System 1**	**System 2**	**System 3**	**System 4**	**System 5**	**System 6**	**System 7**	**System 8**
Specific vulnerability or weakness	●	●	●	●	●	●	●	n/a
Office or organization responsible for resolving the weakness	○	○	●	○	●	●	●	n/a
Estimated funding required to resolve the weakness	○	●	○	○	●	●	○	n/a
Source of the funding required to resolve the weakness	○	○	○	○	○	○	○	n/a
Scheduled completion date for resolving the weakness	●	●	●	○	●	●	●	n/a
Key milestones with completion dates	●	●	●	●	●	●	●	n/a
Changes to milestones and completion dates	◐	◐	●	●	◐	◐	●	n/a
Source that identified the weakness	●	●	●	●	●	●	●	n/a
Status of the corrective action (ongoing, completed, etc.)	●	●	●	●	●	●	●	n/a

Source: GAO analysis of agency data. I GAO-16-501.

Note: ● — generally met; ◐— partially met; ○ — not met; n/a – not applicable

System 8 did not have an active POA&M.

Further, not all of the plans had been periodically updated. For example, remedial actions for systems were past due for four of the eight systems—two each at NASA and OPM.

Without addressing all elements of the POA&M and updating them periodically, agencies may not be able to effectively prioritize and manage their remedial actions and correct known deficiencies in a timely manner.

Not all agencies had developed a continuous monitoring strategy

According to NIST, continuous monitoring facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. As noted earlier, OMB directed agencies to develop and implement an agency-wide information security continuous monitoring strategy in accordance with NIST guidance. NIST recommends that agencies develop a continuous monitoring strategy and implement a program that includes, among other things, (1) organization-defined metrics to be monitored, (2) organization-defined frequencies for monitoring and assessments, (3) ongoing status

monitoring of defined metrics, and (4) reporting of information system security status. Having a continuous monitoring strategy is also required for initial implementation of CDM, which is described earlier in this report.

Three of the four agencies had documented a strategy. However, the strategies did not always include key elements such as metrics to be monitored or frequencies of monitoring the metrics.

- NASA had developed a continuous monitoring strategy. Although the strategy does not specify organization-defined metrics, frequency of monitoring metrics, ongoing status monitoring of metrics, or reporting of security status, other documents address frequency of monitoring. In addition, the agency uses a dashboard that displays ongoing status of metrics such as patching percentages, status of POA&Ms, and upcoming control reviews, among others.
- NRC had included its strategy in a computer security standard. The standard includes a list of what it refers to as "metrics," but the list instead addresses frequency of scanning and testing, and does not include measurable items that could be considered metrics. The standard also addresses reporting of security status, but not ongoing status monitoring.
- OPM had documented metrics to be monitored and had defined frequencies for monitoring and assessments. The agency also had developed a strategy that refers to status monitoring of metrics and reporting of security status.
- VA had developed policy documents that described continuous monitoring, but could not demonstrate that it had developed a strategy.

Without key elements documented in a continuous monitoring strategy, agencies will be at increased risk that they will not be monitoring appropriate metrics at agreed-upon frequencies to aid in agency-wide situational awareness of potential threats and vulnerabilities.

Conclusions

Federal agencies face numerous threats to high-impact systems, with most agencies citing nations as the most serious and most often occurring threat. To help protect against threats, agencies reported existing federal guidance to be useful. In addition, they are in the process of implementing various initiatives, such as CDM, PIV, and NCPS, although the level of implementation varies across the agencies. Although half of the agencies reported that they wanted an expansion of federal initiatives to help protect their high-impact systems, the *Cybersecurity*

Strategy and Implementation Plan generally recognizes these concerns. However, until OMB issues its plans for shared services and security center best practices, agencies will not have the benefit of the efficiency associated with these services and practices to better protect their computing environments.

The four selected agencies had developed, documented, and implemented controls to help protect selected systems. However, weaknesses existed in access controls, including those protecting system boundaries, identifying and authenticating users, authorizing access needed to perform job duties, encrypting sensitive data, and auditing and monitoring system activities. Shortcomings also existed in applying patches to protect against known vulnerabilities, and planning for system contingencies. An underlying reason for these weaknesses is that the agencies had not fully implemented elements of their information security programs. For example, security plans did not always address controls specific to high-impact systems, those with significant security responsibilities did not always complete specialized training, systems' assessments were not comprehensive, and continuous monitoring strategies were incomplete.

Until the selected agencies address weaknesses in access and other controls, including fully implementing elements of their information security programs, the sensitive data maintained on selected systems will be at increased risk of unauthorized access, modification, and disclosure, and the systems at risk of disruption.

Recommendations

To improve security over federal systems, including those considered to be high impact, we recommend that the Director of the Office of Management and Budget issue *Circular A-130*, as well as the plan and practices specified in the *Cybersecurity Strategy and Implementation Plan*.

In addition, to improve agency information security programs, we recommend that the

Administrator of the National Aeronautics and Space Administration take the following five actions:

- Provide and track specialized training for all individuals who have significant security responsibilities.

- Update security assessment plans for selected systems to ensure they include the test procedures to be performed.
- Re-evaluate security control assessments for selected systems to ensure that they comprehensively test technical controls.
- Update remedial action plans for selected systems, to include responsible organization, estimated funding, source of funding, and updated milestones and completion dates.
- Update the continuous monitoring strategy to include metrics, ongoing status monitoring of metrics, and reporting of security status.

Chairman of the Nuclear Regulatory Commission take the following five actions:

- Update security plans for selected systems to ensure that all controls specific to high-impact systems are addressed, including a rationale if the control is not implemented.
- Provide and track specialized training for all individuals who have significant security responsibilities.
- Re-evaluate security control assessments to ensure that they comprehensively test technical controls.
- Update remedial action plans for selected systems, to include responsible organization, estimated funding, funding source, and scheduled completion dates.
- Update the standard that addresses continuous monitoring to include metrics and ongoing status monitoring.

Acting Director of the Office of Personnel Management take the following four actions:

- Update security plans for selected systems to ensure that all controls specific to high-impact systems are addressed, including a rationale if the control is not implemented, and where other plans are cross-referenced, ensure that the other system's plan appropriately addresses the control.
- Provide and track specialized training for all individuals, including contractors, who have significant security responsibilities.
- Re-evaluate security control assessments to ensure that they comprehensively test technical controls.
- Update remedial action plans for selected systems, to include source of funding and updated completion dates.

Secretary of the Department of Veterans Affairs take the following five actions:

- Update security plans for selected systems to ensure that all controls specific to high-impact systems are addressed, including a rationale if the control is not implemented.
- Provide and track specialized training for all individuals who have significant security responsibilities.
- Conduct security control assessments for the two selected systems and ensure the procedures comprehensively test technical controls.
- Update remedial action plans for selected systems, to include estimated funding and funding source.
- Develop a continuous monitoring strategy that addresses organization-defined metrics, frequency of monitoring metrics, ongoing status monitoring of metrics, and reporting of security status.

In four separate reports with limited distribution, we plan to make specific recommendations to each of the four selected agencies to address any weaknesses identified related to boundary protection, identification and authentication, authorization, cryptography, audit and monitoring, patch management, and contingency planning for the selected systems.

Agency Comments and Our Evaluation

We sent draft copies of this report to the 24 agencies included in our survey, as well as OMB and NIST. We received responses from each of the five agencies to which we made recommendations: OMB responded by email and NASA, NRC, OPM, and VA provided written comments which are reprinted in appendices II through V, respectively. The Department of Homeland Security also provided written comments which are reprinted in appendix VI. The Departments of Commerce (including NIST), Defense, Education, Energy, Housing and Urban Development, Interior, Justice, Labor, State, and Transportation; as well as the General Services Administration, Environmental Protection Agency, Social Security Administration, Small Business Administration, and United States Agency for International Development responded in a letter or emails that they had no comments on the draft report. The Department of Health and Human Services provided a technical comment, which we addressed.

In an email sent by our OMB liaison, OMB generally concurred with our recommendation regarding issuance of *Circular A-130*, as well as the plan and practices specified in the *Cybersecurity Strategy and*

Implementation Plan. OMB stated that it recognizes that it must update or draft new cybersecurity policies to provide agencies with sufficient guidance to address the rapidly changing environment, and is in the process of finalizing the first update to A-130 in over 16 years. The agency stated that it has closely collaborated with its interagency partners to develop beneficial cybersecurity services for federal agencies. It also noted the ongoing efforts of the Department of Homeland Security and General Services Administration to increase the use of government-wide shared capabilities for information technology and cybersecurity.

In a letter signed by the Chief Information Officer, NASA concurred with each of our five recommendations. In its response, the agency described actions it plans to take to address the recommendations, including implementation of a commercial tool, as well as expected time frames for completing the actions.

In a letter signed by the Executive Director for Operations, NRC concurred with each of our five recommendations. The commission stated that it will continue to improve its cybersecurity posture by continuing to evaluate the threat environment to ensure the agency's implementation of government security rules and regulations is risk-informed, appropriate, and effective. The commission also provided technical comments, which we considered.

In a letter signed by the Associate Chief Information Officer, OPM concurred with two of our recommendations, partially concurred with a third, and did not concur with a fourth recommendation. OPM concurred with the two recommendations regarding updating the security and remedial action plans for selected systems. OPM partially concurred with our recommendation to provide and track specialized training for individuals, including contractors, who have significant security responsibilities. The office stated it agreed with the intent but not the suggested approach. Instead, OPM noted that it is more appropriate and efficient to monitor training requirements for contractors without access to its network through audits and oversight, as opposed to directly providing and tracking those individuals' training. In prior correspondence, as evidence of its oversight to ensure such training occurred, OPM referred us to the most recent security control assessment for the contractor-operated system we selected. However, in this assessment, to test this particular control, the assessor reviewed policy documents and interviewed two individuals and concluded that the contractor provided annual and refresher training for the employment and operation of environmental controls and the employment and operation of physical

security controls. The procedures performed in testing the control did not ensure that individuals actually completed the training. Without effective tracking (or oversight), OPM is at increased risk that individuals with significant security responsibilities may not have the appropriate training to protect its systems.

OPM did not concur with our recommendation to re-evaluate security control assessments to ensure that they comprehensively test technical controls. The office stated that it had not been provided enough information regarding the technical control findings in order to assess this recommendation. OPM stated that we did not provide the office with sufficient information to evaluate weaknesses that we categorized into topical areas such as boundary protection or authorization, and that we did not provide some information concerning the nature of the weaknesses until a week before this response was due (May 2, 2016). However, we do not believe this is an accurate characterization of the situation. On March 9, 2016, we briefed OPM staff on our technical findings, including how we had categorized them under access controls. As also noted in this report, at that time, we explained that more details regarding these findings, along with associated recommendations, would be reported in a limited distribution report due to the sensitive nature of the information. On March 16, 2016, OPM requested the underlying materials supporting our findings, noting that the ability to review the output of any scans and similar materials would enable OPM to better understand our conclusions. On that same day, we informed agency personnel that they already had all of these materials, as they had provided them to us. We provided a list of all information provided to us for both systems, as well as the names of individuals who had assisted us with our tests. We believe that sufficiently trained technical staff should be able to review such materials and draw the same, or similar, conclusions as we did. We have continued to work with OPM staff to provide clarification where requested. Without comprehensive security control assessments, OPM is at increased risk that it may not detect vulnerabilities in its systems. Therefore, we believe the recommendation is warranted.

In its response, OPM also pointed out that we did not explain in our report that one of the selected systems was contractor-owned and operated. The office stated that this fact is important because it approaches security through contractor oversight, and therefore does not, for example, deploy patches or manipulate administrator passwords itself. We purposefully did not identify the selected system as contractor-owned and operated as to further protect the system's identity. Nevertheless, FISMA requires the

agency to ensure security for information and systems maintained by or on behalf of the agency, including systems used or operated by a contractor or other organization on behalf of the agency. Therefore, although it does not deploy patches for this particular system, for example, OPM is responsible for ensuring that its contractor has such controls in place. OPM noted that it released interim policy on information technology security contract clauses in April 2016, which is intended to improve contractor oversight and enforcement of contract provisions.

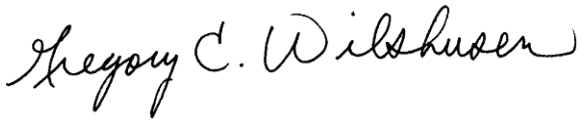
OPM also asserted that it has made improvements to security controls, both at the system level and across its information technology environment, since GAO completed its review of OPM's two systems. OPM noted that these improvements are not reflected in our report. We appreciate OPM's continued efforts to improve its information security. However, our report reflects the state of information security at the time of our review.

In a letter signed by VA's Chief of Staff, VA concurred with our five recommendations. In its response, VA described actions planned and already taken to address the recommendations, as well as expected time frames for completing the actions.

In a letter signed by the Director of the Departmental GAO-OIG Liaison Office, the Department of Homeland Security noted it will continue to move forward to most effectively protect federal civilian agencies, and that its priorities for the year include (1) focusing on continued adoption of the latest version of EINSTEIN by all federal civilian agencies, (2) working with each agency as they deploy the first phase of the Continuous Diagnostics and Mitigation initiative across their networks, and (3) assisting agencies to patch their Internet-facing devices more rapidly.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees; the Secretaries of Homeland Security and Veterans Affairs, the Administrator of the National Aeronautics and Space Administration, the Chairman of the Nuclear Regulatory Commission, the Acting Director of the Office of Personnel Management, the Director of the Office of Management and Budget, and other interested parties. 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 Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@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 VII.



Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati
Chief Technologist

Appendix I: Objectives, Scope, and Methodology

Our objectives were to 1) describe the extent to which agencies have identified cyber threats and reported incidents involving high-impact systems, 2) identify government-wide guidance and efforts to protect these systems, and 3) assess the effectiveness of controls to protect selected high-impact systems at selected federal agencies.

To address objectives one and two, we interviewed officials from the 24 federal agencies[1] covered by the *Chief Financial Officers Act*[2] and the Office of Management and Budget (OMB) for preliminary input on potential questions to include in a survey to the agencies. Considering this input, we developed a web-based survey, which we sent to the agencies to collect, analyze, and summarize data on the cyber threats, security incidents, and security guidance and efforts involving high-impact systems. In our survey, we asked questions about the following topical issues related to systems that agencies categorized as high impact:

- the three most serious (1) threat sources/agents, (2) threat vectors, and (3) common methods of attack affecting their high-impact systems;
- the three (1) sources/agents, (2) threat vectors, and (3) common methods of attack that occur the most often, as indicated, for example, by notifications and alerts;
- the extent challenges impact agency ability to identify cyber threats affecting high-impact systems;
- the usefulness of federal sources in identifying threats affecting high-impact systems;
- the usefulness of existing guidance in protecting high-impact systems; and

[1]The 24 departments and agencies covered by the *Chief Financial Officers Act* are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[2]31 U.S.C. § 901.

- the extent agencies participated in government-wide initiatives and programs, and the usefulness of the initiatives and programs.

To minimize errors from respondents misinterpreting our questions, we pretested the survey with four agencies to ensure the questions were relevant and easy to understand. The selection of agencies for pretesting was based on agency availability. We received survey responses from all 24 agencies from July 20, 2015 to October 8, 2015 with 18 of the 24 agencies reporting having high-impact systems. The survey results represent agency status at the time they responded to the survey. We requested that agency chief information officers and chief information security officers review and confirm the results of the survey. To minimize errors from data processing and analysis, an independent computer specialist verified all programs used to analyze the results.

In addition to the survey, to address our second objective, we examined federal policies and guidance, including United States Computer Emergency Readiness Team (US-CERT) requirements, National Institute of Standards and Technology (NIST) publications,[3] and OMB memorandums.[4] We also reviewed documentation on federal initiatives, such as the Continuous Diagnostics and Mitigation program, Personal Identity Verification, Trusted Internet Connection, and the National Cybersecurity Protection System, DHS's May 2015 Binding Operational Directive,[5] OMB's 30-day Cybersecurity Sprint,[6] the October 2015

[3]National Institute for Science and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, MD: April 2013); *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, MD: February 2010); and *Computer Incident Handling Guide*, SP 800-61, Revision 2 (Gaithersburg, MD: August 2012).

[4]Office of Management and Budget, *M-15-13: Policy to Require Secure Connections across Federal Websites and Web Services* (Washington, D.C.: June 8, 2015); *OMB M-14-03: Enhancing the Security of Federal Information and Information Systems* (Washington, D.C.: Nov. 18, 2013); and *OMB M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Inform*ation (Washington, D.C.: May 22, 2007).

[5]Department of Homeland Security, Binding Operational Directive BOD-15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems* (Washington, D.C.: May 21, 2015).

Cybersecurity Strategy and Implementation Plan,[7] and the recently issued President's *Cybersecurity National Action Plan*.[8] Further, we interviewed officials from the 24 agencies on which organizations had government-wide efforts and guidance assisting agencies. Based on that input, we interviewed officials from OMB, NIST, the Department of Homeland Security's US-CERT, Federal Bureau of Investigation's National Cyber Investigative Joint Task Force, and the Information Security Identity Management Committee on their government-wide efforts and guidance to protect high-impact systems.

To address our third objective, we selected four agencies and two systems at each agency. To select the agencies, we reviewed fiscal year 2014 *Federal Information Security Modernization Act* (FISMA) reports for the 24 federal agencies' reported amount of high-impact systems. We then grouped agencies from the highest to lowest amount of reported high-impact systems, eliminated those agencies that reported having no high-impact systems, and subtracted any national security systems that officials stated were included in their reported FISMA amount. We divided the remaining agencies into quartiles and selected the agency with the highest reported amount of high-impact systems within each quartile. As a result, the agencies selected for our review were the National Aeronautics and Space Administration, Nuclear Regulatory Commission, Office of Personnel Management (OPM), and the Department of Veterans Affairs.

To select the information systems, we asked agencies to provide us with an inventory of their high-impact systems and the categorization of each system in the three security areas of (1) confidentiality, (2) integrity, and (3) availability, as determined by the agency evaluating the system using

[6]Office of Management and Budget, Executive Office of the President, *Fact Sheet: Enhancing and Strengthening the Federal Government's Cybersecurity* (Washington, D.C.: June 12, 2015).

[7]Office of Management and Budget, *OMB M-16-04: Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (Washington, D.C.: Oct. 30, 2015).

[8]The White House, Office of the Press Secretary, *Fact Sheet: Cybersecurity National Action Plan* (Washington, D.C.: Feb. 9, 2016).

Federal Information Processing Standards Publication 199.[9] Based on reviewing the information provided, we selected agency systems that had reported high categorization in all three areas and eliminated any system reviews conducted by their inspectors general. If more than two systems within an agency's inventory were marked as high in the three areas, we narrowed down our selection based on the sensitivity of the data being processed, the system's role in meeting the agency's mission and potential impact to the mission if a security breach were to occur, and location of systems due to resource constraints. After receiving system security documentation from our selected systems, we verified that the overall categorization for the systems' categorization was high. Based on our review of security documentation, we discovered that OPM had inaccurately reported its categorization of two systems in at least one of the three areas due to an error made in transferring data into the agency's inventory tool. Given that OPM's systems remained categorized as high overall, we kept the selected systems within the scope of our review.

To assess the effectiveness of controls at selected agencies for selected systems, we used our *Federal Information Systems Controls Audit Manual*,[10] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information. We also used FISMA, NIST, and OMB standards and guidance, and agency policies and procedures to assess the effectiveness of selected agencies' and systems' information security controls. For each of the eight selected systems, we specifically evaluated controls by conducting the following steps as compared to established guidance, policies, and procedures:

We tested and examined

- whether agencies had appropriately protected system boundaries;

[9]National Institute of Standards and Technology, *FIPS 199: Federal Information Processing Standards Publication, Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, MD: February 2004).

[10]GAO, *Federal Information System Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 2009).

- the complexity, expiration, and policy for passwords on systems and databases to determine if strong password management was being enforced;
- whether the agencies had implemented controls to ensure access to systems was appropriately limited;
- agencies' implementation of encryption to secure sensitive data transmissions on their internal networks;
- whether agencies were sufficiently auditing and monitoring system security events;
- the status of patching for key databases and system components to ensure that patches were up-to-date; and
- continuity of operations planning documentation to determine if such plans had been appropriately documented and tested.

We also reviewed and evaluated agencies' implementation of their information security programs by analyzing

- selected systems' risk assessments to determine whether the assessments were up-to-date, documented, and approved;
- selected systems' security plans to determine the extent to which plans had been reviewed, and included information as required by NIST for high-impact systems;
- training records for individuals with significant IT security-related responsibilities to determine whether they had received specialized training for fiscal year 2015 pursuant to the information tracked;[11]
- security assessment reports for selected systems to determine if the effectiveness of security controls had been periodically assessed; and
- agencies' actions to correct weaknesses for selected systems to determine if they had effectively mitigated or resolved the vulnerability or control deficiency.

[11]We sampled 180 individuals across the four agencies. For each agency reviewed, we developed a list of employees and contractors with potentially significant security responsibilities for the high-impact systems we reviewed. We identified those individuals by (1) examining system security plans, contingency plans, and incident response plans, and (2) including system and database administrators we met with for system testing. We then selected a non-generalizable sample from each list, which resulted in a total sample of 180 employees.

In addition, we interviewed key security representatives and management officials to determine to what extent these information technology controls were in place and to better understand our selected systems' operational environments.

To determine the reliability of the data used to pick our selected agencies and other data used to evaluate controls, we performed an assessment in the following areas:

- number of high-impact systems reported by our four selected agencies in their fiscal year 2014 FISMA report,
- fiscal year 2015 specialized security training records, and
- plans of action and milestones.

We evaluated the materiality of the data to our audit objectives and assessed the data reliability by various means, including reviewing related documents, conducting observations of systems generating data, interviewing knowledgeable agency officials, and reviewing internal controls such as agency policies and procedures. Through a combination of methods, we concluded that the data were sufficiently reliable for the purposes of our reporting objectives.

We conducted this performance audit from February 2015 to May 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the National Aeronautics and Space Administration

National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001

Reply to Attn of: Office of the Chief Information Officer

MAY -3 2016

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems" (GAO-16-501), dated March 31, 2016.

In the draft report, GAO makes the following recommendations addressed to the NASA Administrator intended to improve NASA's information security program:

Recommendation 1: Provide and track specialized training for all individuals who have significant security responsibilities.

Management's Response: Concur. NASA is drafting and finalizing a Role Based Training Implementation Plan. The training will be hosted on the System for Administration, Training, and Educational Resources for NASA (SATERN) Web-based training environment. By implementing this plan, NASA will track specialized training for all individuals who have significant security responsibilities.

Estimated Completion Date: June 30, 2017.

Recommendation 2: Update security assessment plans for selected systems to ensure they include the test procedures to be performed.

Management's Response: Concur. NASA is implementing an RSA Archer solution that includes a Security Assessment and Authorization module. This solution will allow for the update of security assessment plans for NASA systems, to include test procedures. NASA will update the two selected systems security assessment plans by December 9, 2016.

Estimated Completion Date: December 9, 2016.

Recommendation 3: Re-evaluate security control assessments for selected systems to ensure that they comprehensively test technical controls.

Management's Response: Concur. NASA has an Information Assurance Review program in place to review system Security Assessment and Authorization (SA&A) documentation packages. The re-evaluation of the two selected systems security control assessments to ensure comprehensive testing of technical controls will take place under the Information Assurance Reviews.

Estimated Completion Date: September 30, 2016.

Recommendation 4: Update remedial action plans for selected systems, to include responsible organization, estimated funding, source of funding, and updated milestones and completion dates.

Management's Response: Concur. NASA's current Agency-wide Security Assessment and Authorization (SA&A) repository, the Information Technology (IT) Security Center system, includes a Plan of Action and Milestones (POA&M) function to document remedial actions. The current POA&M function does not include all of the requirements outlined for remedial actions. This deficiency will be corrected with the full implementation of the RSA Archer solution for POA&M management. This tool allows the update of remedial action plans for NASA systems, to include responsible organizations, estimated funding, source of funding, and updated milestones and completion dates. NASA will update remedial action plans for the two selected systems by December 9, 2016.

Estimated Completion Date: December 9, 2016.

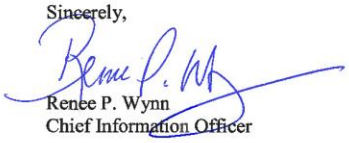
Recommendation 5: Update the continuous monitoring strategy to include metrics, ongoing status monitoring of metrics, and reporting of security status.

Management's Response: Concur. NASA will update the continuous monitoring strategy to include metrics, ongoing status monitoring of metrics, and reporting of security status.

Estimated Completion Date: December 9, 2016.

Once again, thank you for the opportunity to review and comment on this draft report. If you have any questions or require additional information, please contact Ruth McWilliams on (202) 358-5125.

Sincerely,



Renee P. Wynn
Chief Information Officer

Appendix III: Comments from the Nuclear Regulatory Commission

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

April 29, 2016

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
Information Technology
441 G Street, N.W, Room 4488
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the draft of your report GAO-16-501, "Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems," which the U.S. Nuclear Regulatory Commission (NRC) received on March 31, 2016.

The NRC staff has compiled specific comments on the report. These comments are provided in the enclosure.

The U.S. Government Accountability Office (GAO) surveyed 24 Federal agencies with high-impact systems, and tested and evaluated the security controls for 8 high-impact systems at 4 agencies including the NRC. The evaluation of the NRC's performance is consistent with the other 3 Federal agencies. Of the 4 key information security program elements evaluated for the 2 NRC high-impact systems, the NRC met 1 element (risk assessments) and partially met 3 elements (security plans, controls assessment, remedial action plans). The GAO report concludes that:

> Federal agencies face numerous threats to high-impact systems, with most agencies citing nations as the most serious and most often occurring threat. To help protect against threats, agencies reported existing Federal guidance to be useful. In addition, they are in the process of implementing various initiatives, such as Continuous Diagnostics and Mitigation, Personal Identity Verification, and National Cybersecurity Protection System, although the level of implementation varies across the agencies. Although half of the agencies reported that they wanted an expansion of federal initiatives to help protect their high-impact systems, the Cybersecurity Strategy and Implementation Plan generally recognizes these concerns. However, until the Office of Management and Budget issues its plans for shared services and security center best practices, agencies will not have the benefit of the efficiency associated with these services and practices to better protect their computing environments.

G. Wilshusen - 2 -

The NRC's comments on the recommendations are listed below:

- GAO Recommendation: Update security plans for selected systems to ensure that all controls specific to high-impact systems are addressed, including a rationale if the control is not implemented.

  NRC Response: The NRC agrees with GAO's recommendation. The security plans for the selected systems are currently being reviewed and updated as part of our reauthorization and the continuous monitoring activities as outlined by agency policy. As a part of this exercise, all controls specific to high-impact systems are being addressed as recommended.

- GAO Recommendation: Provide and track specialized training for all individuals who have significant security responsibilities.

  NRC Response: The NRC agrees with GAO's recommendation. The NRC is validating the current list of staff required to receive training, verifying that existing contracts require the periodic training given by the NRC, and engaging multiple management levels to ensure that required training is attended.

- GAO Recommendation: Re-evaluate security control assessments to ensure that they comprehensively test technical controls.

  NRC Response: The NRC agrees with GAO's recommendation. The NRC is examining GAO's findings along with NRC assessments to identify areas where NRC assessments can be improved. The NRC has also recently implemented a new enterprise vulnerability/configuration scanning tool that has enhanced the agency's ability to perform comprehensive system technical control assessments and support ongoing continuous monitoring activities.

- GAO Recommendation: Update remedial action plans for selected systems, to include responsible organization, estimated funding, funding source, and updated completion dates.

  NRC Response: The NRC agrees with GAO's recommendation. The NRC has applied additional resources to support the review and to update and continue managing the remedial action plans for the selected systems.

- GAO Recommendation: Update the standard that addresses continuous monitoring to include metrics and ongoing status monitoring.

  NRC Response: The NRC agrees with GAO's recommendation. The NRC is reviewing the continuous monitoring process and will be updating the process to include additional continuous monitoring metrics.

The NRC will continue its efforts to improve our cybersecurity posture. We recognize that Federal agencies face numerous threats to high-impact systems. We will continue to evaluate the current threat environment to ensure that NRC implementation of government information

G. Wilshusen - 3 -

security rules and regulations is risk-informed, appropriate, and effective. Should you have any questions concerning these comments, please contact John Jolicoeur at 301-415-1642.

Sincerely,

Victor M. McCree
Executive Director
for Operations

Enclosure:
NRC Comments on the Draft
Government Accountability Office
Report (GAO-16-501)

Appendix IV: Comments from the Office of Personnel Management

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

MAY 0 2 2016

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

Dear Mr. Wilshusen:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, Agencies Need to Improve Controls over Selected High-Impact Systems, GAO-16-501, Job Code Number 100064.

GAO conducted a review of two OPM systems in October 2015, identified in the Report as System 5 and System 6. We note at the outset that OPM has continued to make security improvements and mitigate issues, both at the system level and across the entire OPM IT environment, since that time, and that these security improvements are not reflected in the GAO's final report. OPM has welcomed and been receptive to evaluation and feedback from a variety of sources, including from its interagency partners such as the Department of Homeland Security, as well as OPM's Office of the Inspector General, and has already implemented changes that have strengthened our cybersecurity posture. While OPM appreciates the analysis performed by GAO, OPM also notes below several areas where we believe additional information is necessary in order to place the Report's findings in the proper context. Responses to your specific recommendations are also provided below.

System Ownership and Responsibilities

The GAO Report fails to explain that OPM System 6 is an external, contractor-owned and contractor-operated system located outside of OPM's network. OPM believes this context is necessary, because it means that OPM approaches security of this system through contractor oversight and enforcement of the provisions of its contract, including enforcement of FISMA as incorporated through the contract. Although OPM has responsibility for security of the system and System 6 is a system in OPM's inventory, OPM does not have custody or control over the system and so does not, for example, deploy patches or manipulate administrator passwords itself. OPM also notes that the vendor for OPM System 6, at the time of the GAO engagement, was under contract to provide document conversion services to OPM. However, the vendor is no longer under contract to provide conversion services at this time and the system has been disconnected. While OPM is in the process of working towards a new contract, no corrective activities or action will or can be performed related to the GAO findings until there is a new contract in place.

1

www.opm.gov Recruit, Retain and Honor a World-Class Workforce to Serve the American People www.usajobs.gov

As a general note, and in line with separate GAO and OMB guidance and consistent with government-wide efforts in this area, OPM also recently released an interim policy and is currently in the process of releasing new IT security contract clauses that is a step towards remediating GAO's findings and enabling OPM to improve its oversight of IT security and FISMA compliance in its contracts. On April 25, 2016, OPM released an interim policy on IT security contract clauses which will be immediately included in all applicable IT/IT related procurement actions that have not yet been awarded, as well as those existing contracts considered by program offices in consultation with their IT Project Managers, of high-risk. This will aid in OPM's effort to improve contractor oversight and enforcement of contract provisions. System 6 will be audited within a year of being under contract to provide conversions services to OPM.

Lack of Specificity Regarding Certain Findings

OPM also notes that the GAO has failed in some cases to provide OPM with sufficient information about its findings to enable the OPM to either verify the existence of the alleged deficiency, or remediate the alleged deficiency. Although OPM repeatedly sought clarification on these questions from GAO prior to the issuance of the Report, OPM at this time is still unable to either confirm or refute certain findings, based on a lack of critical supporting detail and information from GAO.

Most significantly, the GAO Report states that "one or more control weaknesses" exist in Systems 5 and 6, and that this unspecified quantity of weaknesses fall into broad categories such as "authorization" or "boundary protection" (*see* Table 8). Although OPM received some information concerning the nature of the weaknesses GAO identified, GAO did not provide it until less than a week before this response was due and OPM is still awaiting further clarification from GAO on some topics. The information OPM requested would permit verification or remediation of the weaknesses, such as the host name or IP addresses where the weakness was found, the scope of each weakness, a recommendation for remediation of the weakness, or what evidence would support a validation that the weakness had been remedied. Without timely access to this information, which OPM typically receives from other auditors that look at OPM systems, OPM has been unable to either verify the accuracy of GAO's findings, or demonstrate whether they have been remediated, as of the time of this response.

OPM does note, however, that it has improved security controls in these areas since the audit. OPM has instituted a layered defense to intrusion that is a substantial defense for most risk. In addition, OPM now has a robust logging management system and security audit logging. OPM is working to deploy a new automated tool that will provide enhanced support for documenting its security controls as well as the inheritance of controls from one system to another. Moreover, with respect to certain findings, GAO acknowledged that the manner in which OPM was approaching a topic was sufficient even though GAO might prefer a different method.

For OPM owned and operated systems, OPM has implemented multi-factor authentication at the network access level for privileged and non-privileged users and is also working towards multi-factor authentication at the application level in order to create multiple layers of security. As far as other mitigation strategies for access controls, OPM implements two-factor authentication for

system administration access and activity is monitored via a privileged identity monitoring solution. Meanwhile, OPM has a new enterprise patch management solution that is being implemented. On the process front, OPM is putting into practice a new incident response plan, and periodically requests independent penetration testing from our interagency partners. OPM has also implemented network access controls that prevent access by non-government furnished equipment. More generally, OPM continues to collaborate with our interagency partners and the Office of Inspector General on ways to bolster our cyber defenses.

Although OPM is committed to undertaking remediation efforts to address GAO's findings, it has been impeded in its efforts to do so due to this lack of clarity and specificity from GAO that would aid in those efforts. To the extent that GAO provides specific information about its findings, OPM has and will continue to take corrective action. OPM will also continue its own efforts to review and remediate on a system-wide level.

RESPONSE TO GAO RECOMMENDATIONS

Recommendation 1: Update security plans for selected systems to ensure that all controls specific to high-impact systems are addressed, including a rationale if the control is not implemented, and where other plans are cross-referenced, ensure that the other system's plan appropriately addresses the control.

Response: We concur. OPM will migrate security plans into an automated system which will allow for improved management of security controls. The automated system will provide enhanced capabilities to support the security control overlay process, including documenting rationale when a decision is made for not implementing certain controls, as well as capturing details of security controls that are inherited from other OPM systems and programs.

Recommendation 2: Provide and track specialized training for all individuals, including contractors, who have significant security responsibilities.

Response: We partially concur. While OPM agrees with the intent of the recommendation, OPM does not agree with the approach suggested by GAO during the evaluation. Contractors working on OPM System 5 must have access to the OPM network, and are tracked by OPM. If there is a contractor that does not access the OPM network, there are clauses set forth in the contract to require the contractor to meet OPM training requirements. It is OPM's position that it is more appropriate and efficient for OPM to monitor IT training requirements for contractors without access to OPM's network through contractor audits and oversight, as opposed to directly providing and tracking those individuals' training. OPM's IT Security Office currently conducts annual site visits on a sample of contractor sites each year, and is working to improve the site assessment process to better align it to verify compliance with all of the standard IT contract clauses, including those regarding contractor employee training.

OPM will issue a new Security Awareness and Training policy to improve upon the existing policy and reinforce the training requirements. OPM will also release updated IT contract clauses covering security training requirements. OPM will enhance its oversight and enforcement of the training requirements established in the policy and contract clauses as well.

Recommendation 3: Re-evaluate security control assessments to ensure that they comprehensively test technical controls.

Response: We do not concur. At the time of this response, OPM has not been provided enough information regarding the technical control findings to fully respond to this recommendation. Additionally, the recommendation as written does not address the issues identified within the technical assessment and suggests another cause for which no analysis was conducted and / or provided to OPM for review.

OPM will hold follow-up meetings with GAO to allow for full review of the technical findings and will then apply any remediation for those findings, as appropriate.

OPM is also in the process of establishing a new contract vehicle for the performance of security assessment services. The contracts will be managed by the Cybersecurity program to allow for greater oversight of the quality of security control assessments.

Recommendation 4: Update remedial action plans for selected systems, to include source of funding and updated completion dates.

Response: We concur. OPM will update the Plan of Action and Milestones (POA&M) for the selected systems to provide new completion dates for unresolved weaknesses and will include the source of funding for the system as a part of the POA&M report.

We appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Cord Chase, 202-606-0117, and Cord.Chase@opm.gov.

Sincerely,

David A. Vargas, MSA, CPA
Associate Chief Information Officer
U.S. Office of Personnel Management

4

Appendix V: Comments from the Veterans Administration

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

May 5, 2016

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

Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***"INFORMATION SECURITY: Agencies Need to Improve Controls over Selected High-Impact Systems"*** (GAO-16-501). VA generally agrees with GAO's conclusions.

The enclosure sets forth the action to be taken to address the GAO draft report recommendations.

Sincerely,

Robert D. Snyder
Chief of Staff

Enclosure

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
"INFORMATION SECURITY: Agencies Need to Improve Controls over Selected High-Impact Systems"
(GAO-16-501)

GAO Recommendation: To improve agency information security programs, GAO recommends that the Secretary of Veterans Affairs take the following five actions:

Recommendation 1: update security plans for selected systems to ensure that all controls specific to high-impact systems are addressed, including a rationale if the control is not implemented.

VA Comment: Concur. A check of the selected systems verified that all High Impact Security Controls have been addressed. The security controls are currently addressed in various System Security Plans as the accreditation boundaries are based on platform and application. All High Impact Security Controls are addressed within these plans. By the second quarter of fiscal year (FY) 2017, the System Security Plan will include all controls in one plan. Target Completion Date: March 2017.

Recommendation 2: provide and track specialized training for all individuals who have significant security responsibilities.

VA Comment: Concur. All role-based training is tracked in VA's Talent Management System (TMS). The VA memorandum "Mandatory Role-Based Training" dated February 23, 2012, (Attachment A) states assignments are a one-time requirement and supervisors have the ability to assign or request the employee to take additional role-based training when required. New Office of Information and Technology (OI&T) staff and employees that change roles are automatically assigned a role-based curricula based on their functional role within TMS. The IT Workforce Development (ITWD) organization will provide monthly OI&T staff role-based training curricula deficiency reports to OI&T leadership for required action. Target Completion Date: late-May 2016.

Recommendation 3: Conduct security control assessments for the two selected systems, and ensure the procedures comprehensively test technical controls.

VA Comment: Concur. VA's internal Security Control Assessment (SCA) team has begun to perform SCAs on every system in VA's Federal Information Security Management Act of 2002 inventory. The two systems in question are on the schedule for the first quarter of FY 2017. Target Completion Date: December 2016.

Recommendation 4: update remedial action plans for selected systems, to include estimated funding and funding source.

VA Comment: Concur. VA follows Office of Management and Budget requirements for proper Plan of Actions and Milestones (POAM) management. Funding requirements are captured in our Government, Risk and Compliance tool. All open POAMs for the

Enclosure

Department of Veterans Affairs (VA) Response to
Government Accountability Office (GAO) Draft Report
"INFORMATION SECURITY: Agencies Need to Improve Controls over Selected High-Impact Systems"
(GAO-16-501)

selected systems have estimated financials entered. The closed findings have been updated with regard to final financials. Data for remedial action plans for these systems has been updated. Attachment B shows the collective financials to support closing this recommendation. Target Completion Date: Completed.

Recommendation 5: develop a continuous monitoring strategy that addresses organization-defined metrics, frequency of monitoring metrics, ongoing status monitoring of metrics, or reporting of security status.

VA Comment: Concur. VA redefined its Information Security Continuous Monitoring (ISCM) capabilities by defining the solutions, products, and services administered by the Department to continuously monitor VA assets. In March 2016, VA's ISCM approach was reviewed by industry experts, and recommendations to enhance the Department's capabilities were provided. Those recommendations were incorporated into the Agency's Enterprise Cyber Security Strategy. As part of that strategy, a new ISCM framework will be developed that addresses the people, processes, technology, and performance monitoring mechanisms identified in the ISCM Maturity Model. Target Completion Date: August 2016.

Appendix VI: Comments from the Department of Homeland Security

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

Homeland Security

April 28, 2016

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

Re: Draft Report GAO-16-501, "INFORMATION SECURITY: Agencies Need to Improve Controls over Selected High-Impact Systems"

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

As Secretary of Homeland Security Jeh Johnson has said, "Cybersecurity is one of the most important missions of DHS. Cybersecurity is homeland security."

The Department is pleased to note GAO's positive recognition that the United States Computer Emergency Readiness Team (US-CERT) was identified as the most useful public or private resource for identifying potential cyber threats by the 18 federal agencies surveyed during this audit. The draft report also highlighted that agencies identified several other DHS services as helpful in improving the cybersecurity of their high-impact systems, including the Continuous Diagnostics and Mitigation (CDM) program, the National Cybersecurity Protection System (NCPS), US-CERT monthly operational bulletins, and CyberStat reviews.

DHS' National Protection and Programs Directorate (NPPD) serves a critical role in homeland security by leading the national effort to secure and enhance the resilience of the Nation's infrastructure against cyber and physical risks. NPPD works with interagency partners as well as owners and operators of critical infrastructure in the private sector and state, local, tribal, and territorial government agencies to, collectively, maintain, secure, functioning, and resilient infrastructure that is vital to public confidence and the Nation's safety, prosperity, and well-being.

Cybersecurity is a shared responsibility and we all are more secure when our systems are secure. We are all truly connected and a vulnerability for one can create a problem for many. NPPD will continue moving forward to most effectively protect federal civilian agencies. Its priorities this year include:

- focusing on continued adoption of EINSTEIN 3A by all federal civilian agencies, as required by the Cybersecurity Act of 2015;
- working with each agency as they deploy CDM Phase 1 tools across their networks; and
- assisting agencies to patch their vulnerabilities in Internet-facing devices increasingly more rapidly through recurring scans and clear, actionable metrics.

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

2

Appendix VII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, WilshusenG@gao.gov
Nabajyoti Barkakati, Ph.D., (202) 512-4499, BarkakatiN@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Edward Alexander, David Hayes, Jeffrey Knott, Harold Lewis, and Duc Ngo (assistant directors); Angela Bell; Bruce Cain; Sa'ar Dagani; Jennifer R. Franks; Nancy Glover; Myong Kim; Linda Kochersberger; Sean Mays; Kevin Metcalfe; David Plocher; Dana Pon; Brandon Sanders; and Eugene Stevens made key contributions to this report. Carl Barden, Christopher Businsky, Debra Conner, Wilfred Holloway, Stuart Kaufman, Carl Ramirez, and Christine San also provided assistance.