United States Government Accountability Office

Report to Congressional Committees

August 2017

INFORMATION SECURITY

OPM Has Improved Controls, but Further Efforts Are Needed

Accessible Version

GAO-17-614

August 2017

INFORMATION SECURITY

OPM Has Improved Controls, but Further Efforts are Needed

GAO Highlights

Highlights of GAO-17-614, a report to congressional committees

Why GAO Did This Study

OPM collects and maintains personal data on millions of individuals, including data related to security clearance investigations. In 2015, OPM reported significant breaches of personal information that affected 21.5 million individuals.

The Senate report accompanying the *Financial Services and General Government Appropriations Act, 2016* included a provision for GAO to review information security at OPM. GAO evaluated OPM's (1) actions since the 2015 reported data breaches to prevent, mitigate, and respond to data breaches involving sensitive personnel records and information; (2) information security policies and practices for implementing selected government-wide initiatives and requirements; and (3) procedures for overseeing the security of OPM information maintained by contractors providing IT services. To do so, GAO examined policies, plans, and procedures and other documents; tested controls for selected systems; and interviewed officials. This is a public version of a sensitive report being issued concurrently. GAO omitted certain specific examples due to the sensitive nature of the information.

What GAO Recommends

GAO is making five recommendations to improve OPM's security. OPM concurred with four of these and partially concurred with the one on validating its corrective actions. GAO continues to believe that implementation of this recommendation is warranted. In GAO's limited distribution report, GAO made nine additional recommendations.

View GAO-17-614. 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

Since the 2015 data breaches, the Office of Personnel Management (OPM) has taken actions to prevent, mitigate, and respond to data breaches involving sensitive personal and background investigation information, but actions are not complete. OPM implemented or made progress towards implementing 19 recommendations made by the United States Computer Emergency Readiness Team (US-CERT) to bolster OPM's information security practices and controls in the wake of the 2015 breaches. GAO determined that the agency completed actions for 11 of the recommendations and took actions for the remaining 8, with actions for 4 of these 8 requiring further improvement (see table). In addition, OPM did not consistently update completion dates for outstanding recommendations and did not validate corrective actions taken to ensure that the actions effectively addressed the recommendations.

Table 1: GAO Assessment of the Status of Recommendations to the Office of Personnel Management (OPM) by the U.S. Computer Emergency Readiness Team

Status	Number of Recommendations
Completed actions	11
Further improvements needed for actions OPM considered complete	4
In progress	4

Source: GAO evaluation of OPM data. | GAO-17-614

OPM also made progress in implementing information security policies and practices associated with selected government-wide initiatives and requirements. However, it did not fully implement all of the requirements. For example, OPM identified its high value assets, such as systems containing sensitive information that might be attractive to potential adversaries, but it did not encrypt stored data on one selected system and did not encrypt transmitted data on another. Until OPM completes implementation of government-wide requirements, its systems are at greater risk than they need be.

OPM's procedures for overseeing the security of its contractor-operated systems did not ensure that controls were comprehensively tested. Although the agency has implemented elements of contractor oversight such as recording security assessment findings for contractor-operated systems in remediation plans, it did not ensure that system security assessments involved comprehensive testing. The agency requires information system security officers to conduct quality assurance reviews that include reviewing security assessments of contractor-operated systems; however, its policy did not include detailed guidance on how the reviews are to be conducted. Until such a procedure is clearly defined and documented, OPM will have less assurance that the security controls intended to protect OPM information maintained on contractor-operated systems are sufficiently implemented.

Contents

Tables

Abbreviations

CAP Goals	Cross-Agency Priority Goals
CDM	Continuous Diagnostics and Mitigation
CIO	chief information officer
CISO	chief information security officer
CSIP	*Cybersecurity Strategy and Implementation Plan*
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOD	Department of Defense
FIPS	federal information processing standards
FISMA	*Federal Information Security Modernization Act*
ISCM	information security continuous monitoring
ISSO	information system security officer
NBIB	National Background Investigations Bureau
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
PIV	personal identity verification
POA&M	plans of action and milestones
SP	special publication
US-CERT	United States Computer Emergency Readiness Team

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

August 3, 2017

The Honorable Shelley Moore Capito
Chairman
The Honorable Christopher Coons
Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations
United States Senate

The Honorable Tom Graves
Chairman
The Honorable Mike Quigley
Ranking Member
Subcommittee on Financial Services and General Government
Committee on Appropriations
House of Representatives

Cyber incidents at federal agencies demonstrate the damage that increasingly sophisticated cyber threats can cause and underscore the importance of effectively protecting federal systems. In June 2015, the Office of Personnel Management (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 compromised its systems and the files related to background investigations for 21.5 million individuals. Improving the security over federal systems is imperative to protecting the confidentiality, integrity, and availability of the information on federal systems, including that considered to be personally identifiable information (PII).[1]

Since 1997, we have designated the security of information on federal systems (i.e., information security) to be a government-wide high-risk area. In 2003, we expanded the area to include computerized systems

[1]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.

supporting the nation's critical infrastructure and in 2015, we included protecting the privacy of PII.[2]

In light of the breaches at OPM, the Senate report accompanying the *Financial Services and General Government Appropriations Act, 2016* includes a provision for us to review information security at OPM.[3] Our objectives were to evaluate OPM's (1) actions since the 2015 data breaches to prevent, mitigate, and respond to data breaches involving sensitive personnel records and information; (2) information security policies and practices for implementing selected government-wide initiatives and requirements; and (3) procedures for overseeing the security of OPM information maintained by contractors providing information technology services.

This report is a public version of a sensitive report that we issued concurrently. Because sensitive information about systems' operating environments or shortcomings could potentially be exploited, this report omits sensitive information about OPM's systems. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

To address the first objective, we examined information security policies, plans, and procedures, as well as other relevant documents; performed testing of OPM's internal network and software tools; and interviewed officials to determine the extent to which the agency had implemented recommendations made by the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT) in light of the breach. We also met with officials and reviewed documentation pertaining to the status of OPM's National Background Investigation Bureau (NBIB).

For the second objective, we examined policies, plans, and procedures, as well as other relevant documents, and interviewed officials from the OPM Office of the Chief Information Officer (OCIO) to determine the

[2]For our latest high-risk report, see GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[3]Senate Report No. 114-97 (July 30, 2015), accompanying the *Financial Services and General Government Appropriations Act, 2016*, Div. E, Pub. L. No. 114-113 (Dec. 18, 2015); 129 Stat. 2242, 2423.

extent to which the agency had implemented requirements associated with key government-wide initiatives. We focused on the security controls agencies are required to implement as described in the October 2015 *Cybersecurity Strategy and Implementation Plan* (CSIP)[4] and the Cybersecurity Cross-Agency Priority (CAP) Goals.[5]

We also collected new information by reviewing relevant controls on three systems. We selected these systems based on the agency categorizing them as high-impact[6] systems and them not being recently audited by GAO. Because system weaknesses identified in this report could be exploited, we are not identifying the systems' names or other specifics related to our selection. In a separate report with limited distribution, we provide more details regarding our scope and methodology.

For the third objective, we reviewed policies and security control assessments for three contractor-operated systems. We selected the two active, contractor-operated systems that were not involved in the breach, but were categorized by the agency as high-impact systems. We also selected one active system that the agency categorized as a moderate-impact system.[7] These three systems had also undergone a recent system security assessment.

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

[5]Cybersecurity goals were established by the prior administration as part of implementing the requirement in the *Government Performance and Results Act Modernization Act of 2010* to develop federal government priority goals for information technology management. Sec. 5, Pub. L. No. 111-352 (Jan. 4, 2011); 124 Stat. 3866, 3873; 31 U.S.C. § 1120(a)(1)(B).

[6]A high-impact system is a system in which 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. National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199 (Gaithersburg, MD: February 2004).

[7]A moderate-impact system is one in which the loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. For example, it might cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced. National Institute of Standards and Technology, FIPS Publication 199.

We focused the scope of our review on assessments of moderate- and high-impact controls in the following National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53[8] defined control families: access controls, audit and accountability, security assessment and authorization, configuration management, contingency planning, risk assessments, and system and information integrity. In addition, we excluded controls identified by the assessors as either inherited or not applicable.[9] See appendix I for additional details on our objectives, scope, and methodology.

We conducted this performance audit from January 2016 to August 2017 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

OPM collects and maintains personal information on millions of individuals, including sensitive security clearance data. The agency is the central human resources agency for the federal government, overseeing all policy to support federal agencies' human resources departments—from classification and qualifications systems to pay, leave, and benefit policies. In addition, the agency provides investigative products and services for more than 100 federal agencies to use as the basis for suitability for employment and security clearance determinations. It also provides more than 95 percent of the government's background investigations, conducting approximately 2.2 million investigations a year. The agency had a fiscal year 2016 discretionary budget authority of about $245 million and around 5,300 full-time equivalent employees.

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

[9]Inherited controls, also referred to as common controls, provide a security capability for multiple information systems within an organization. When common controls are used to support a specific information system, they are referenced by that specific system as an inherited control.

On June 4, 2015, OPM reported that a breach to its information technology systems and data had potentially compromised the personal information of about 4.2 million former and current federal employees. In July 2015, OPM reported that a separate but related cyber incident targeting its databases containing background investigation records was estimated to have compromised security clearance background information of about 21.5 million individuals. In the months that followed the breach, further investigation by the agency revealed that the information compromised as a result of these breaches included employee Social Security numbers, residency and education history, employment history, information about immediate family and other personal and business acquaintances, criminal and financial history, job assignments, performance ratings, training information, and the fingerprints of approximately 5.6 million individuals. An estimated 22.1 million individuals had some form of PII stolen, with 3.6 million being a victim of both breaches.

OPM's director is responsible for ensuring the adequacy of the agency's information security program, including information security policies, procedures, and practices. The OPM Chief Information Officer (CIO) leads the development, management, operations, and support of the IT infrastructure, with the assistance of the managers and staff in OCIO. The agency's Chief Information Security Officer (CISO) serves as the CIO's primary information security adviser and guides the information security activities of the agency's authorizing officials and information security officers. OPM also has a Management Review Board, which includes the CISO, Deputy CISO, and certain branch chiefs as members. This board is intended to manage information security risks by reviewing and approving the creation and closure actions associated with plans of action and milestones (POA&M), which address identified weaknesses.

Federal Law Establishes Security Requirements to Protect Federal Information and Systems

The *Federal Information Security Modernization Act* (FISMA) *of 2014*[10] is intended to provide a comprehensive framework for ensuring the

[10]The *Federal Information Security Modernization Act of 2014* (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 both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

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. FISMA assigns responsibility to the head of each agency for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. The law also delegates to the agency CIO (or comparable official) the authority to ensure compliance with FISMA requirements.

FISMA also 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, including those provided or managed by another agency, contractor, or other source. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and procedures; developing 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; developing and implementing procedures for detecting, reporting, and responding to security incidents; and ensuring continuity of operations. In addition, FISMA requires agencies to comply with NIST standards and the Office of Management and Budget (OMB) requires agencies to comply with NIST guidelines. Further, FISMA requires the operation of a central federal information security incident center, a role now filled by the DHS's US-CERT.

US-CERT Has a Role in Strengthening Agency Information Security Programs

The mission of US-CERT is to strive for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world. This mission is reflected in the four critical activities it is responsible for carrying out:

- Providing cybersecurity protection to federal civilian executive branch agencies through intrusion detection and prevention capabilities.

- Developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal, and territorial governments; critical infrastructure owners and operators; private industry; and international organizations. Some of the information currently distributed includes weekly vulnerability bulletins and technical alerts.
- Responding to incidents and analyzing data about emerging cyber threats.
- Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.

US-CERT has developed programs and resources to carry out these activities, including the distribution of technical alerts, tips, and weekly vulnerability bulletins. In addition, it occasionally performs reviews at the agency and system levels, an activity that allows it to provide agencies more detailed information on agency- and/or system-specific weaknesses, vulnerabilities, and actions to remediate them.

Government-wide Cybersecurity Initiatives Have Been Established

OMB has established various initiatives intended to protect federal systems. These include, but are not limited to, OMB's 30-day Cybersecurity Sprint,[11] the October 2015 CSIP, and the CAP Goals. Agency participation and compliance with these key initiatives, which are outlined in table 1, are mandatory.

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

Table 1: Key Government-wide Cybersecurity Initiatives by Date and Description

Government-wide initiatives	Date	Description
Continued Implementation of Homeland Security Presidential Directive 12 (M-11-11)	2/3/2011	This Office of Management and Budget (OMB) directive requires federal agencies to follow DHS's plan of action guidance for compliance with *Homeland Security Presidential Directive 12* requirements, which includes the creation of a mandatory, government-wide standard issued by the federal government to its employees and contractors for secure and reliable forms of identification, including the use of multifactor authentication.
Enhancing the Security of Federal Information and Information Systems (M-14-03)	11/18/2013	This OMB memorandum provides agencies with guidance for managing information security risk on a continuous basis and builds on efforts, such as those related to continuous monitoring, to achieve the cybersecurity cross-agency priority goals.
Cross-Agency Priority Goals (CAP Goals)	3/4/2014	The CAP Goals were established by OMB and are intended to address longstanding cybersecurity challenges through, among other things, ongoing awareness of information security, vulnerabilities, and threats and enacting the administration's top cybersecurity capabilities and directives, to include those related to continuous monitoring, least privileged access, anti-malware technology, and multifactor authentication.
30-day Cybersecurity Sprint (Cyber Sprint)	6/12/2015	This initiative by OMB instructed federal agencies to take immediate actions—to include the use of multifactor authentication, ensuring least privileged access, and the deployment of Department of Homeland Security threat indicators—to further improve their cybersecurity and protect information and assets against evolving threats that target the nation's cyber infrastructure.
Cybersecurity Strategy and Implementation Plan (CSIP)	10/30/2015	This plan issued by OMB contains initiatives aimed at strengthening federal civilian cybersecurity and is the result of a comprehensive review of federal cybersecurity policies, procedures, and practices. The goals include addressing critical cybersecurity gaps and emerging priorities, such as the deployment of existing and emerging technologies and practices (e.g. multifactor authentication, least privileged access, patch management, continuous monitoring, and the deployment of DHS threat indicators) and the creation of a high value assets list.
Revised Managing Federal Information as a Strategic Resource (OMB A-130)	7/28/2016	This OMB circular establishes general policy for planning, budgeting, governance, acquisition, and management of federal information (e.g. establishing requirements related to data encryption), personnel, equipment, funds, IT resources, and supporting infrastructure and services.

Source: GAO analysis of federal initiatives. I GAO-17-614

Prior GAO Recommendations Aimed to Improve OPM's Information Security

In August 2014, we issued a report[12] that examined federal agency oversight of contractor-operated federal IT systems. We reported that OPM, one of six federal agencies reviewed, had generally established

[12]GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, GAO-14-612 (Washington, D.C.: Aug. 8, 2014).

security and privacy requirements and had planned for assessments to determine the effectiveness of contractor implementation of controls. However, the system assessments performed were not always effective. We recommended that OPM improve its oversight of contractor testing to ensure that tests are being fully executed for all contractor-operated systems. According to OPM officials, efforts are underway to implement the recommendation.

In May 2016, we reported[13] on the implementation of OPM's information security program and the security of selected high-impact systems. We reported that OPM, one of four agencies reviewed, had implemented numerous controls to protect selected systems, but access controls had not always been implemented effectively. Weaknesses also existed in patching known software vulnerabilities and planning for contingencies. An underlying reason for these weaknesses was that OPM had not fully implemented key elements of their information security program. We recommended that OPM fully implement key elements of its program, including addressing shortcomings related to its security plans, training, and system testing. According to OPM officials, the agency is in the process of taking actions to address these recommendations.

In addition, we issued a restricted version[14] of the May 2016 report that identified vulnerabilities specific to each of the two systems we reviewed and made recommendations to resolve access control weaknesses in those systems. In December 2016, OPM indicated its concurrence with the recommendations and provided time frames for implementing them.

OPM Has Made Progress in Improving Its Security to Prevent, Mitigate, and Respond to Breaches, but Efforts Are Not Complete

Since the 2015 data breaches, OPM has made progress in improving its security to prevent, mitigate, and respond to data breaches involving sensitive personal records and background investigations information.

[13]GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

[14]GAO, *Information Security: OPM Needs to Improve Controls over Selected High-Impact Systems*, GAO-16-687SU (Washington, D.C.: Aug. 15, 2016).

After breaches of personnel and background investigation information were reported, US-CERT worked with the agency to resolve issues and develop a comprehensive mitigation strategy. Toward this end, in September 2015, US-CERT made 19 recommendations to OPM to help the agency improve its overall security posture and, thus, improve its ability to protect its systems and information from security breaches.

As of May 2017, OPM had fully implemented 11 of the recommendations. For the remaining 8 recommendations, actions for 4 were still in progress. For the other 4 recommendations, OPM indicated that it had completed actions to address them, but we noted further improvements were needed. Further, OPM had not validated actions taken to address the recommendations in a timely manner.

Beyond actions associated with the US-CERT recommendations, OPM established a new organization—the National Background Investigation Bureau (NBIB)—to perform background investigation services. It signed a memorandum of agreement with the Department of Defense (DOD) to develop and secure new systems to support the bureau's mission.

OPM Has Made Progress Implementing US-CERT Recommendations, but Actions Remain

OPM has made progress in implementing the 19 US-CERT recommendations, but has opportunities to improve on the actions it has taken. As shown in table 2 and subsequently discussed, the agency completed actions for 11 recommendations; needed to further improve on actions taken for 4 other recommendations it indicated had been completed; and needed to complete actions in progress for the remaining 4.

Table 2: GAO Assessment of Office of Personnel Management (OPM) Efforts to Address U.S. Computer Emergency Readiness Team (US-CERT) Recommendations

US-CERT recommendation	GAO assessment
1	Needs further action
2	In Progress
3	Needs further action
4	Completed
5	Completed
6	In Progress
7	Needs further action
8	Completed
9	Completed
10	Completed
11	Completed
12	Completed
13	Completed
14	Completed
15	Needs further action
16	In Progress
17	Completed
18	Completed
19	In Progress

●—Completed actions

◕—Further improvements needed for actions OPM considered complete

◑—In progress

Source: GAO analysis of OPM data. I GAO-17-614

Due to the sensitive nature of the recommendations, we are not providing the specific recommendations or specific examples associated with them. Generally, the recommendations pertained to strengthening activities and controls related to passwords, access permissions, patches, audit and monitoring, among other things.

OPM Did Not Effectively Monitor Actions Taken to Address the US-CERT Recommendations

OMB requires agencies to create a POA&M to track efforts to remediate identified weaknesses, such as those leading to the 19 recommendations made by US-CERT. In addition, OPM's policy requires that scheduled completion dates be included in the plan. The policy also requires a

system's Information System Security Officer (ISSO) to develop a weakness closure package containing evidence of how items in the POA&M have been remediated before the issue (recommendation in this case) can be closed. The policy further requires that the closure package be reviewed by the Management Review Board, which approves closure.

Although OPM has a POA&M[15] to address the 19 recommendations, it had not updated completion dates in the plan. The POA&M showed scheduled completion dates of either October or December 2015 for all recommendations. However, a separate recommendation tracking document provided to us indicated a planned completion date in the third quarter of 2017 for at least one recommendation. With such inconsistencies and lack of updates, OPM's ability to gauge performance is limited.

Further, the agency had not validated in a timely manner its actions to implement the recommendations. For example, the plan indicated that all actions to address at least 7 of the 19 recommendations had been completed in September or October 2015. However, as of April 2017, at least 17 months later, OPM had not reviewed closure packages or otherwise validated the effectiveness of the actions taken to implement these recommendations. OPM OCIO officials explained that the Management Review Board, at a December 2016 meeting, had discussed the expected evidence required to demonstrate formal closure. In addition, they noted that the US-CERT recommendations in the POA&M would not be closed out until evidence was collected to validate the actions taken.

While the intent to validate evidence of remediation actions is commendable, the length of time OPM has taken to do so is troubling in light of the cybersecurity incidents at the agency and given the heightened risk environment in which it operates. Because the US-CERT recommendations are intended to improve the agency's security posture, more timely validation of the effectiveness of the actions taken is warranted. Until closure packages are created and the evidence of such actions is validated, OPM has limited assurance that the actions taken have effectively mitigated vulnerabilities that can expose its systems to cybersecurity incidents.

[15]In this case, OPM generated a report from its database of POA&Ms for the US-CERT recommendations. The report included, for each recommendation, a list of actions to be completed in order to implement the given recommendation.

OPM Established the National Background Investigations Bureau to Help Improve Security Since the Breach

In addition to its actions to address the US-CERT recommendations in response to the breaches that affected background investigation data, OPM updated roles and responsibilities for handling background investigations. Following the recommendation of a 90-day suitability and security interagency review that identified changes needed to strengthen the background investigation process, in January 2016, the administration announced its plans to create the NBIB within OPM. As of October 2016, OPM had transferred responsibility for performing personnel background investigations from its old Federal Investigative Services unit to NBIB and entered into a memorandum of agreement with DOD to develop and operate information systems supporting the bureau.

According to the bureau's fact sheet, NBIB is intended to:

- improve the security of background investigation IT systems through a partnership with DOD,
- improve access to criminal history records through the creation of a law enforcement liaison unit,
- improve the automation and management of background investigation records,
- improve the efficiency of background investigation business processes, and
- consolidate the management of federal and contract field operations.

According to OPM OCIO officials, existing background investigation information systems and data will continue to be maintained at OPM while DOD designs and develops a new system to support NBIB. OPM plans to maintain the legacy data for historical and reporting purposes once the new system is operational. At this time, the legacy background investigation system is expected to operate for another 3 years or until all cases in it can be closed out.

To support future NBIB operations, the Defense Information Systems Agency (DISA) is in the initial stages of designing the new system, DOD OCIO officials said. While OPM will remain the owner of the background investigations data and processes, DISA will build, operate, and secure the National Background Investigation System, according to the memorandum of agreement between the agencies. According to the DOD

officials, the primary benefit of having DISA host and operate the system is that it will be able to take advantage of DOD's existing information security controls to help ensure the security of the system.

OPM Made Progress Addressing Policies and Practices Associated with Key Government-wide Initiatives and Requirements, but Had Not Fully Implemented All of Them

OMB's CSIP and CAP Goals require federal agencies, including OPM, to take specific cybersecurity actions to bolster their system security. The requirements include identifying high value assets, minimizing the number of privileged users, using multifactor authentication to access resources, limiting the access privileged accounts have, using data encryption at rest and in transit, deploying DHS cyber threat indicators,[16] using anti-phishing and anti-malware technology, and subjecting systems to continuous monitoring. Of the eight required actions we selected for review, OPM had developed and documented specific policies that addressed seven of them, had fully implemented two, and had taken actions to partially implement the remaining six. Until OPM completes implementation of the government-wide requirements, its systems are at greater risk than they need be.

[16]The *Cybersecurity Information Sharing Act of 2015,* Div. N, Title I, Sec. 102(6), Pub. L. No. 114-113 (Dec. 18, 2015) defines threat indicators as information that is necessary to describe or identify: (a) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (b) a method of defeating a security control or exploitation of a security vulnerability; (c) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (d) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (e) malicious cyber command and control; (f) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (g) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (h) any combination thereof.

OPM Identified Its High Value Assets

High value assets refer to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical federal operations; or house unique collections of data (by size or content), making them of particular interest to criminal, politically-motivated, or state-sponsored actors. According to CSIP,[17] federal agencies must continue to identify and submit a list of high value assets to DHS.

OPM had developed, documented, and implemented an information security policy for identifying its high value assets. For example, OPM's policy stated that, as a part of its security authorization process, a security categorization of its information systems shall be conducted to include an evaluation to determine if a system will be a high value asset. The ISSO is responsible for documenting those systems identified as being high value assets using prescribed templates.

Further, OPM had taken action to identify its high value assets. To do this, according to OCIO officials, the agency considered factors such as 1) Federal Information Processing Standards (FIPS) Publication 199 categorization of high impact; 2) the sensitivity of system information; 3) the amount of PII; and 4) the size, location, and mission of a system. By identifying a list of its high value assets, OPM is better positioned to quickly identify and initiate efforts to protect its high value assets from imminent danger of a cybersecurity attack.

OPM Implemented Actions to Minimize the Number of Certain Privileged Users, but Not for Others

According to CSIP, privileged users refer to those users with a network account with elevated privileges that is typically allocated to system administrators, network administrators, database administrators, and others who are responsible for system/application control, monitoring, or administration functions—functions and responsibilities beyond the control of ordinary users. Cyber Sprint and CSIP require federal agencies

[17]M-16-04.

to tighten policies and practices for privileged users by inventorying and minimizing the number of privileged users.

OPM defined the scope of its privileged users and implemented a process for inventorying privileged accounts. The agency's policy defines users with elevated privileges as being those users who are authorized to perform security-relevant functions that ordinary users are not authorized to perform.

OPM demonstrated that it reduced the number of network administrators; however, the agency had not minimized other types of accounts with elevated privileges. To ensure privileged access is required for these other types of accounts, OPM OCIO officials explained that the agency conducts periodic reviews of accounts and that this review consists of ensuring that privileged access for these accounts is still warranted. However, the agency could not provide any artifacts to demonstrate this process, other than periodic reporting of the number of privileged users.

Establishing policy and minimizing the number of network administrators is a positive step. However, until OPM demonstrates that privileged access for other relevant accounts is warranted, increased risk exists that individuals may have access privileges not required to perform their job.

OPM Required Multifactor Authentication to Its Network, but Not to Two Other Systems Reviewed

Multifactor authentication—the use of more than one of the combinations of the following factors: something you know (e.g., a password), something you have (e.g., an identification badge), or something you are (e.g., a fingerprint or other biometric)—is a stronger form of authentication than single-factor authentication. According to OMB M-11-11,[18] existing physical and logical access control systems must be upgraded to use personal identity verification (PIV) credentials, in accordance with NIST guidelines. In 2015, the Cyber Sprint required agencies to "dramatically accelerate" the use of a PIV card or alternative form of multifactor authentication for access to information systems, and CSIP requires agencies to complete implementation. Further, the CAP Goal requires

[18]Office of Management and Budget, *Continued Implementation of Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors*, M-11-11 (Washington, D.C.: Feb. 3, 2011).

agencies to implement a set of capabilities that ensure the use of multiple factors to authenticate to information technology resources. NIST states that agencies can satisfy certain identification and authentication requirements by complying with the requirements in *Homeland Security Presidential Directive 12*[19] and using multifactor authentication, such as PIV cards.[20]

OPM had developed and documented information security policies for implementing multifactor authentication, such as enforcing the use of PIV cards. For example, OPM's policy states that multifactor authentication is required for network and local access for privileged and non-privileged accounts and the use of the cards is required to gain access to information systems, when feasible.

OPM had implemented the use of PIV cards on one of three systems we reviewed. However, it did not require or implement the use of PIV cards or other multifactor authentication methods for the two other systems. According to OPM OCIO officials, the agency plans to complete implementation of PIV cards for all systems no later than 2018.

In its fiscal year 2016 FISMA audit report, OPM's Office of the Inspector General (OIG) reported that it had validated the agency's implementation of network-level multifactor authentication based on a prior recommendation. However, the OIG reported that only 2 of OPM's 46 major systems (applications)[21] were compliant with OMB requirements related to PIV authentication, and recommended that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multifactor authentication using PIV credentials. The

[19]*Homeland Security Presidential Directive 12*, issued in August 2004, directed the establishment of a mandatory, government-wide standard for secure and reliable forms of identification for federal government employees and contractors that access government-controlled facilities and information systems.

[20]NIST defines a personal identity verification card as a physical artifact (e.g., identity card or "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, or digitized fingerprint representation) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable).

[21]According to OMB, a major information system is a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

office concurred with the recommendation and stated that it would work to continue the implementation of an initial enterprise identity and access management solution for enforcing multifactor authentication, including the use of PIV credentials where feasible and appropriate. OPM officials indicated in the report that they were working towards multifactor authentication at the system level in order to create multiple layers of security, but that implementation efforts are ongoing.

Until OPM upgrades all of its information systems to require the use of multifactor authentication mechanisms like PIV cards, its systems and applications may be susceptible to attack if an attacker compromises its network. Because we consider these actions to be in progress, we are not making a recommendation at this time.

OPM Controlled the Access of Privileged User Accounts, but Additional Actions are Needed

To further protect systems, agencies should employ the principle of least privilege. This principle involves granting users the most restrictive set of privileges needed to perform authorized tasks. One CAP Goal specifies that agencies should implement a set of capabilities that ensures users have access to only those resources that are required for their job function. Further, the Cyber Sprint initiative and CSIP require agencies to tighten policies and practices for privileged users by, to the greatest extent possible, limiting functions that users can perform when using privileged accounts and ensuring that privileged user activities are logged and that such logs are reviewed regularly.

OPM has developed, documented, and partially implemented an information security policy that incorporated the principle of least privilege. For example, OPM's policy requires that users with privileged accounts only use these accounts for security-related functions and use non-privileged accounts for other system functions. The policy also requires that privileged user activities be logged and reviewed regularly. OPM initiated efforts to implement this policy; however, it has not been fully implemented. Due to the sensitive nature of the recommendation and the actions needed to implement it, these details are provided in a separate report with limited distribution.

OPM's Implementation of Data Encryption Varied for Selected Systems

Encryption of data can be used to 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 (in transit) or stored (at rest) data. According to OMB Circular A-130,[22] when the assessed risk indicates the need, agencies must encrypt federal information at rest and in transit unless otherwise protected by alternative physical and logical safeguards implemented at multiple layers, including networks, systems, applications, and data. It notes that agencies must apply encryption to federal information categorized as either moderate or high impact in accordance with FIPS Publication 199 unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their mission, functions, or operations.

OPM has developed, documented, and partially implemented an information security policy relevant to data encryption. For example, OPM policy requires system owners to ensure that moderate- and high-impact information systems and PII are protected using data encryption at rest and in transit in accordance with FIPS 140-2.[23]

Nevertheless, OPM's implementation of data encryption at rest and in transit varied for the three systems we reviewed. Specifically,

- One system was not configured to encrypt data in transit, but its production database was configured to encrypt data at rest.
- The second system was configured to encrypt data in transit, but was not configured to encrypt data at rest.
- For the third system, encryption efforts were nearly complete as of March 2017, and the agency was working to complete this effort. Accordingly, we are not making a recommendation at this time.

[22]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 28, 2016).

[23]National Institute of Standards and Technology, *Federal Information Processing Standard: Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-2 (Gaithersburg, MD: May 2001).

Until OPM fully deploys encryption for the selected systems, the agency will be at increased risk that the confidentiality and integrity of the data in transit and stored on its systems is not fully protected.

OPM Took Steps to Deploy Threat Indicators

Threat indicators play a key role in creating shared situational awareness of malicious cyber activity. According to the Cyber Sprint initiative, agencies must immediately deploy indicators provided by DHS regarding priority threat-actor techniques, tactics, and procedures to scan systems and check logs. In addition, CSIP states that, on an ongoing basis, agencies must scan for indicators of compromise within 24 hours of receipt of the threat indicators from DHS. Further, the *Standards for Internal Control in the Federal Government* state that management is to document in policies the internal control responsibilities of the organization.[24] The standards further state that controls be documented; documentation of controls is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

Although OPM had deployed DHS threat indicators and scanned for them, its policy had not been updated for this specific requirement. The agency had developed and documented a policy that describes threat indicators such as signatures.[25] For example, OPM's information security handbook states that signatures related to malware should be updated. The agency also had a procedure in place that gives the CISO responsibility for ensuring that security alerts and advisories are received on a continuous basis, and notes that scanning will occur periodically. However, neither the policy nor procedure described responsibilities for ensuring the 24-hour scanning requirements are accomplished and monitored. By updating the policy and procedure to specifically document roles and responsibilities associated with DHS threat indicator requirements, such as scanning, OPM could further improve upon its ability to ensure that controls are being communicated to those

[24]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[25]According to NIST, a signature is a recognizable, distinguishing pattern that can be associated with an attack, such as a binary string of characters in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

responsible for their performance and are capable of being monitored and evaluated.

OPM Used Several Anti-Malware and Anti-Phishing Technologies, but Shortcomings Existed

Anti-phishing and malware defense is important to protect agencies from phishing attempts, where attackers use social engineering with 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. According to the CAP Goal for anti-phishing and malware defense, agencies must implement technologies, processes, and training that reduce the risk of malware introduced through e-mail and malicious web sites.

OPM had deployed several anti-malware technologies, but shortcomings existed with the tools deployed. Due to the sensitive nature of the types of tools deployed and any shortcomings, we are not providing specific examples in this report. This information is provided in a separate report with limited distribution.

OPM also implemented an effective training exercise to reduce the risk of malware introduced through e-mail and malicious websites. At the request of OPM, DHS's National Cybersecurity Assessment and Technical Services conducted e-mail phishing exercises to assess the agency's potential risk and vulnerabilities to e-mail phishing attacks. Over the course of months, OPM showed improvement with results from the phishing exercises. Specifically, in April 2016, DHS reported that it had sent 3,000 fictitious e-mails with a link that would redirect users to a website that describes the dangers of clicking on untrusted links. Of the 3,000 e-mails, 366 unique users (about 12 percent) clicked on the phishing link. Subsequent testing indicated that users were better informed. In September 2016, for the 882 suspicious e-mails sent over the course of 7 campaigns, DHS reported only one instance (less than 1 percent) of a user clicking on a phishing link. By having personnel better informed to detect phishing attempts, OPM has greater assurance that agency systems will not be compromised by such a threat.

OPM Did Not Assess Selected Systems According to Its Continuous Monitoring Plan

Continuous monitoring is an important activity in assessing the security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation. According to NIST, continuous monitoring facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The CAP Goal for Information Security Continuous Monitoring (ISCM) states that agencies should provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness. Additionally, OMB Memorandum 14-03[26] requires federal agencies to develop and maintain an ISCM strategy and establish an ISCM program.

Further, to facilitate continuous monitoring by agencies, DHS established the Continuous Diagnostics and Mitigation (CDM) program. The program involves the delivery of tools and services intended 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 the agency and federal levels. CSIP states that federal agencies are to accelerate the implementation of capabilities and tools to identify risks to their systems and networks, including DHS's CDM program. Further, NIST SP 800-53 recommends that an organization provide role-based security training to personnel with assigned security roles and responsibilities.

OPM had established an ISCM program and took actions to implement continuous monitoring practices. The agency also developed a continuous monitoring strategy that requires system owners to assess security controls for ongoing continuous monitoring of its information systems based on the established security control assessment frequencies specified in the continuous monitoring plan. According to the agency's fiscal year 2016 continuous monitoring plan, owners are to assess specified controls on each system periodically according to the schedule in the plan.

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

However, OPM did not consistently assess the security controls at defined frequencies for the three selected systems we reviewed. For example, the agency did not assess the controls for the systems for several months at a time. According to OPM OCIO officials, security controls for two systems were not assessed in accordance with defined frequencies due to a shortage of ISSOs at the agency, and the other system was not assessed because the system was undergoing reauthorization. However, until OPM consistently performs periodic assessments of the selected systems, the agency will have less assurance of whether controls for these systems are effective and operating as intended.

In its 2016 FISMA report, the OIG identified a weakness in OPM's information security governance regarding the extremely high employee turnover rate for the ISSO positions and OPM's lack of filling those positions. Subsequently, the OIG recommended that OPM hire a sufficient number of ISSOs to adequately support all of the agency's major information systems. The agency concurred with the recommendation and indicated that plans were in place to hire a sufficient number of ISSOs to support all of its major information systems.

OPM deployed continuous monitoring tools obtained through DHS's CDM program, and developed and deployed its own internal continuous monitoring dashboard. Officials stated that the agency completed the first phase[27] of DHS's CDM program and is in the process of implementing the second phase.

However, OPM has not issued role-based training requirements for the individuals configuring and maintaining the deployed CDM tools. OCIO officials told us the agency drafted role-based training requirements for CDM users, but could not demonstrate to us that it has done so.

Until OPM develops and implements role-based training requirements for staff using its CDM tools, it will not be able to ensure that staff are using the tools properly. As a result, the usefulness of the tools for monitoring the security of the agency's information systems may be diminished.

[27]The CDM program covers 15 continuous diagnostic capabilities. The first phase of CDM focuses on endpoint integrity: management of hardware and software assets, configuration management, and vulnerability management, which are foundational capabilities to protect systems and data. Phases 2 and 3 are being further defined to include identity and infrastructure management.

OPM's Procedures for Overseeing the Security of its Contractor-Operated Systems Did Not Ensure that Controls Were Comprehensively Tested

OPM has implemented elements of contractor oversight such as recording security assessment findings for contractor-operated systems in remediation plans, but it did not ensure that system security assessments involved comprehensive testing. The agency requires ISSOs to conduct quality assurance reviews that include reviewing security assessments of contractor-operated systems; however, its policy did not include detailed guidance on how the reviews are to be conducted.

OPM Has Not Ensured that Security Control Assessments for Contractor-Operated Systems Are Comprehensive

To determine the effectiveness of contractors' implementation of federal information security requirements, agencies rely on security control assessments for contractor-operated systems. FISMA requires that agencies periodically test the management, operational, and technical controls for their systems, including for those systems that are operated by a contractor of an agency or other organization on behalf of an agency. In addition, NIST SP 800-53 recommends that agencies assess systems to determine if controls are implemented correctly, operating as intended, and producing the desired results. It also requires that a plan be developed that describes the assessment procedures to be used to determine security control effectiveness, and that the agency produce a report that contains the results of this assessment. Further, NIST SP 800-53A[28] contains a suggested methodology for control assessments, including personnel to interview, documents to examine, and testing to be performed. It also states that different assessment methodologies may be used as long as they are sufficient to identify weaknesses.

[28]National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Special Publication 800-53A, Revision 4 (Gaithersburg, MD: December 2014).

OPM ensured that security control assessments had been conducted for the contractor-operated systems we selected for review; however, instances existed where the methodology employed to conduct the assessments was not sufficient to identify potential weaknesses. Specifically, third-party assessors, on behalf of OPM's contractors, recently conducted security assessments for each of the three contractor-operated systems we reviewed.[29] The methodologies for the assessments included document examinations, interviews, and system testing.

We determined that many of the selected controls[30] had been properly assessed, as shown in table 3.

Table 3: Evaluation of Controls Assessed for Selected Contractor-Operated Systems

System	Number of controls in assessments reviewed by GAO	Number of controls satisfactorily assessed	Number of controls unsatisfactorily assessed	Number of controls with insufficient information
System 1	120	97	23	0
System 2	108	105	3	0
System 3	86	8	0	78

Source: GAO analysis of selected security control assessments. I GAO-17-614

The assessors had addressed most controls for at least two systems satisfactorily; nevertheless, shortcomings existed in the completeness of the testing of specific controls. For example, for System 1, 23 of the 120 controls we reviewed had not been properly assessed. For the 23 controls, the assessor did not test the system to determine if the controls were in place. In addition, for System 3, the security control assessment provided few details on the procedures used to evaluate the effectiveness of the system's security controls. Instead, the assessors recorded the exact same procedures for every control, and few had enough detail in the results to determine if the assessors had employed sufficient procedures.

[29]The three systems selected for this objective are different from the three systems selected for our second objective.

[30]To evaluate the assessments, we selected controls from the following NIST 800-53 control families: access control, audit and accountability, security assessment and authorization, configuration management, contingency planning, risk assessment, and system information and integrity. The number of controls varied between systems because certain controls were not applicable for each system.

OPM has developed, documented, and implemented a process for overseeing the security of contractor-operated systems. The process involved reviewing the third-party security control assessments, but it did not ensure the comprehensiveness of the assessments. OPM has established a quality assurance process that includes reviewing security control assessments.[31] This process consisted of a standard form letter that the ISSO completes after reviewing the assessment package provided by the third-party assessor. For all three selected contractor-operated systems, security officers completed the letter and noted shortcomings with the security control assessments:

- System 1: the ISSO noted some problems due to a lack of provided evidence. For example, the assessor concluded that a number of controls were partially satisfied, despite evidence not being provided by the contractor to the assessor.
- System 2: the security officer identified documentation issues with several controls. For example, the system security plan described the system inconsistently with other documents, such as the contingency plan.
- System 3: the ISSO stated that most of the evidence provided by the assessor was not referenced to the specific procedures performed.

Nevertheless, the security officers did not comment on the comprehensiveness of testing, such as the scope and depth of testing by the third-party assessors. In February 2017, OPM issued an updated authorization guide, which stated that the security officer should review the assessment results and evidence and conduct a quality assurance review on the procedures executed by the independent assessor. However, the guide does not include instructions on how the security officer should perform this review. Until OPM provides more detailed guidance to the ISSOs, the ISSOs may not conduct a rigorous review of the assessment. Therefore, the agency will have less assurance that the security controls for its contractor-operated systems are comprehensively assessed.

[31]The process covers an entire security assessment and authorization package. According to NIST, a security assessment and authorization package contains the security plan, security assessment report, plan of action and milestones, and other documentation deemed necessary by the official responsible for authorizing the operation of the system.

We have previously made recommendations related to OPM's procedures for ensuring the sufficiency of security control assessments for its systems, including those operated by contractors on its behalf. In our August 2014 report related to agency oversight of information technology contractors, we recommended that the agency develop, document, and implement oversight procedures for ensuring that a system test is fully executed for each contractor-operated system.[32] The agency concurred with the recommendation, but, as of April 2017, had not provided evidence that the recommendation had been implemented.

Further, in our May 2016 report related to the security of high-impact systems, we recommended that OPM reevaluate security control assessments to ensure that they comprehensively test technical controls for two selected high-impact systems, one of which was a contractor-operated system.[33] The agency did not concur with our recommendation. However, without comprehensive security control assessments for these systems, OPM is at increased risk that it may not detect vulnerabilities in the systems. Therefore, we believe the recommendation is warranted.

OPM Has Developed and Documented Remedial Action Plans for Weaknesses Identified During Security Assessments

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 an information system. NIST recommends that agencies develop a POA&M for an information system to document the agency's planned remedial actions to correct identified weaknesses.

OPM developed a POA&M for each of the three reviewed systems and recorded 63 of 64 security weaknesses identified in security assessments for those systems. Tracking the weaknesses that arise from security assessments allows OPM to keep track of the weaknesses as they are remediated or their risk is accepted. Table 4 shows the number of security weaknesses per system reviewed.

[32]GAO-14-612.

[33]GAO-16-501.

Table 4: Inclusion of Identified Security Weaknesses in Plans of Actions and Milestones (POA&M)

System	Number of identified weaknesses in assessments reviewed by GAO	Number of weaknesses included in the POA&M	Number of weaknesses not included in the POA&M
System 1	8	7	1
System 2	52	52	0
System 3	4	4	0

Source: GAO analysis of selected security control assessments and plans of action and milestones. I GAO-17-614

OPM policy also requires management oversight and review of remediation plans. Contractors are to provide evidence, which is to be reviewed and approved by multiple parties at OPM before a POA&M is considered closed. However, because the assessments we selected were so recent, we were unable to evaluate whether this process had been effectively implemented.

Conclusions

OPM collects and maintains highly sensitive personal information on millions of individuals, including sensitive security clearance data. Cyber incidents at OPM demonstrated the impact that increasingly sophisticated cyber threats can cause and underscore the importance of protecting the agency's systems. OPM has improved its security posture and is in the process of taking numerous actions, such as addressing recommendations from US-CERT and implementing government-wide requirements and initiatives that could decrease the risk of future security breaches if effectively implemented. However, by not validating remedial actions in a timely manner, the agency has limited assurance whether these actions effectively mitigated vulnerabilities that can expose systems to incidents. In addition, OPM had not consistently updated milestones for outstanding US-CERT recommendations or complied with its own plan for conducting periodic control assessments. Also, training needed to ensure proper use of monitoring tools was not being completed because the agency has not documented such requirements. Further, key security controls on selected contractor-operated systems have not always been comprehensively tested. Until OPM further improves controls over its information and information systems, it has limited assurance that sufficient security controls are in place and operating as intended.

Recommendations for Executive Action

To further improve security over personnel and other sensitive information at the agency, we are recommending that the Acting Director of OPM implement the following five recommendations:

1. Update the POA&M to reflect expected completion dates for implementing the recommendations made by US-CERT.
2. Improve the timeliness of validating evidence associated with actions taken to address the US-CERT recommendations.
3. Update policy to reflect deployment of DHS threat indicators and the specific 24-hour scanning requirement.
4. Develop and implement role-based training requirements for staff using CDM tools.
5. Provide detailed guidance on the quality assurance process that includes evaluating security control assessments.

In a separate report with limited distribution, we are making nine recommendations to the Acting Director to improve upon actions taken to implement the recommendations made by US-CERT and to further implement government-wide requirements.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from OPM. In its comments, which are re-printed in appendix II, the agency concurred with four of our five recommendations and partially concurred with one recommendation.

OPM partially concurred with our recommendation that it improve the timeliness of validating evidence associated with actions taken to address the US-CERT recommendations. The agency did not specifically address the reason for its partial concurrence, but stated that it will review its management practices to support more timely closure of POA&Ms. Regardless of whether OPM reviews its management practices, performing timely validation of evidence is critical. As noted in this report, at least 17 months had passed without OPM validating evidence that it had effectively implemented the US-CERT recommendations. Until the evidence is validated, OPM will have limited assurance that the actions

taken have mitigated vulnerabilities that can expose its systems to cybersecurity incidents.

In addition, OPM provided comments concerning the approach of our audit and aspects of our report message. In particular, the agency stated that GAO did not fully acknowledge OPM's "defense in depth" strategy and that the report does not present a fully accurate picture of the agency's cybersecurity posture. As we state in this report, our objectives were to evaluate OPM's actions taken since the 2015 breach, implementation of requirements associated with selected government-wide initiatives, and oversight of contractor-operated systems. We designed and performed audit procedures to collect sufficient evidence to accomplish these objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Beyond the results of this audit, we previously reported in 2016 that OPM needed to improve security controls over its high-impact systems that we selected for review. In two prior reports, we made numerous recommendations to enhance the agency's information security program[34] and to resolve access control weaknesses in those systems.[35] To date, these recommendations remain open. Based on the results of our prior work and this audit, we believe our current report appropriately reflects OPM's cybersecurity posture, consistent with our audit objectives.

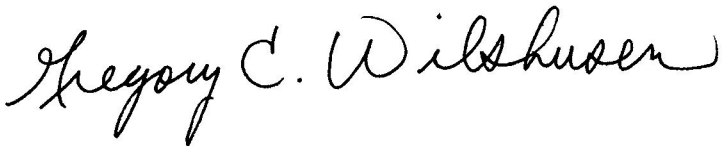
OPM also indicated that it has taken steps to enhance its cybersecurity posture in multiple areas through the addition of cybersecurity tools and security updates, staff and agency-wide training, critical personnel hiring, and collaboration with its interagency partners. We agree that these are positive actions. Effective implementation of these actions and our recommendations is essential to ensuring that sufficient security controls are in place and operating as intended.

We are sending copies of this report to appropriate congressional committees, the acting Director of the Office of Personnel Management, including its Office of the Inspector General, and other interested congressional parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

[34]GAO-16-501.

[35]GAO-16-687SU.

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 III.



Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati
Chief Technologist

Appendix I: Objectives, Scope, and Methodology

Our objectives were to evaluate the Office of Personnel Management's (OPM) 1) actions since the 2015 data breaches to prevent, mitigate, and respond to data breaches involving sensitive personnel records and information; 2) information security policies and practices as they relate to selected government-wide initiatives and requirements; and 3) procedures for overseeing the security of OPM information maintained by contractors providing information technology services.

To address the first objective, we assessed the extent to which the agency had implemented 19 recommendations that the United States Computer Emergency Response Team (US-CERT) made in its 2015 breach investigation report. We chose to focus on the status of US-CERT's recommendations for this objective in order to avoid duplication of effort. According to US-CERT, its recommendations outlined mitigations and security best practices based on the specific compromise and OPM's cybersecurity environment, and are tailored to the OPM environment.

To determine the extent of implementation and whether further improvements were needed, we reviewed the status (e.g., complete or in progress) of OPM's actions to address the recommendations made by US-CERT. We focused on one or more actions described in the plans of action and milestones provided to us. We interviewed officials from OPM's Office of the Chief Information Officer (OCIO) and reviewed the agency's information security documentation, to include policies, plans, and procedures. We also performed limited testing of the agency's internal network and software tools to determine the extent to which US-CERT's recommendations had been implemented. This testing included examining system and device configurations, firewall rules, system status reports, and account listings. We focused on those software tools that OPM indicated it had deployed as actions taken to implement US-CERT recommendations. If, after reviewing the plans provided by OPM and performing our own testing, we could not account for a specific recommendation or disagreed with the implementation status, we followed up with the agency.

For this objective, we evaluated the reliability of the data related to the number of workstations at OPM, as well as the number of outstanding

patches. We 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. We concluded that the data were sufficiently reliable for the purposes of this reporting objective.

As part of this objective, because the data breaches involved background investigation information, we also reviewed OPM's plans to establish the new National Background Investigations Bureau (NBIB), its plans to transfer the information systems supporting NBIB to the Department of Defense (DOD), and DOD's plans for the National Background Investigations System. To accomplish this, we reviewed the memorandum of agreement between the agencies and implementation plans and interviewed officials from OPM and DOD.

To address the second objective, we focused on the security controls agencies are required to implement, as described in the Office of Management and Budget's October 2015 *Cybersecurity Strategy and Implementation Plan*[1] (CSIP) and the Cybersecurity Cross-Agency Priority (CAP) Goals.[2] In addition, OMB issued an updated version of its Circular A-130,[3] which we also reviewed. Based on our review of these documents, we determined that government-wide requirements associated with them include: 1) identifying high value assets, 2) minimizing the number of privileged users, 3) using multifactor authentication, 4) limiting the access for privileged accounts, 5) using data encryption, 6) deploying cyber threat indicators issued by the Department of Homeland Security, 7) using anti-phishing and anti-malware technology, and 8) subjecting systems to continuous monitoring. Further, we reviewed and applied the National Institute of Standards and

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

[2]Cybersecurity goals were established by the prior administration as part of implementing the requirement in the *Government Performance and Results Act Modernization Act of 2010* to develop federal government priority goals for information technology management. Sec. 5, Pub. L. No. 111-352 (Jan. 4, 2011); 124 Stat. 3866, 3873; 31 U.S.C. § 1120(a)(1)(B).

[3]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 28, 2016).

Technology's (NIST) standards and guidelines[4] that are related to these requirements.

To determine the extent to which OPM had implemented the requirements associated with the initiatives, we reviewed agency policies, implementation plans, and other related documents, and interviewed OPM OCIO officials and contractors. We verified this information and collected new information by reviewing relevant controls on three selected systems. We selected these systems based on the agency categorizing them as high-impact[5] systems and them not being recently audited by GAO. Because system weaknesses identified in this report could be exploited, we are not identifying the system names or other specifics related to our selection. In a separate report with limited distribution, we provide more details regarding our scope and methodology. The review we conducted was targeted to acquire information specifically related to this objective and was therefore not comprehensive in nature. Some of the testing we performed included reviewing configuration settings, administrative account privileges and authorizations, and data encryption.

To address our third objective, we interviewed OPM officials and reviewed OPM policy and system security assessments. For selected OPM contractor-operated systems, we reviewed the system's security assessments to determine whether the security control review conducted by the assessor was adequate to evaluate the effectiveness of the controls tested. We selected the two active, contractor-operated systems that were not involved in the breach, but were categorized by the agency as high-impact systems. We also selected one active system that the

[4]For example, National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems,* Federal Information Processing Standards Publication 200 (Gaithersburg, MD: March 2006) and *Security and Privacy Controls for Federal Information Systems and Organizations,* Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013).

[5]A high-impact system is a system in which 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. National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199 (Gaithersburg, MD: February 2004).

agency categorized as moderate impact.[6] Because system weaknesses identified in this report could be exploited, we are not identifying the systems' names or other specifics related to our selection. We focused the scope of our review on assessments of moderate- and high-impact controls in the following NIST Special Publication (SP) 800-53 defined control families: access controls, audit and accountability, security assessment and authorization, configuration management, contingency planning, risk assessments, and system and information integrity. In addition, we excluded controls identified by the assessors as either inherited or not applicable.[7]

We determined the sufficiency of the procedures used by comparing the requirements and recommended testing procedures—as defined in NIST SP 800-53 and NIST SP 800-53A[8]—of each control with the testing procedures documented by assessors in the assessment results. For each control, we evaluated whether the type (e.g., interview, observation, technical testing) and scope of the testing performed was such that one could accurately determine whether a given control had been effectively implemented. We also reviewed the plans of action and milestones associated with each assessment to determine whether the assessment results were reflected in the plans.

We conducted this performance audit from January 2016 to August 2017 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.

[6]A moderate-impact system is one in which the loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. For example, it might cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced. National Institute of Standards and Technology, FIPS Publication 199.

[7]Inherited controls, also referred to as common controls, provide a security capability for multiple information systems within an organization. When common controls are used to support a specific information system, they are referenced by that specific system as an inherited control.

[8]National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Special Publication 800-53A, Revision 4 (Gaithersburg, MD: December 2014).

Appendix II: Comments from the Office of Personnel Management

Chief Information Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

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, OPM Information Security, GAO-17-614, Job Code Number 100559.

OPM appreciates GAO's recognition of our significant progress in several information security areas. OPM has taken steps to enhance its cybersecurity posture in multiple areas through: the addition of cybersecurity tools and security updates; staff and agency-wide training; hiring critical personnel; and collaboration with OPM's interagency partners. OPM recognizes that cybersecurity is not just about technology, but is also about people. Therefore, in addition to strengthening technology, OPM has added seasoned cybersecurity and IT experts to an already talented team. OPM continues to leverage and utilize interagency partnerships and the expertise of the IT and cyber communities across government.

OPM welcomes and is receptive to the evaluation and feedback from GAO, as with other oversight entities, continuously drives to improve and enhance information security at OPM, and continues to implement changes that strengthen OPM's cybersecurity posture.

While OPM appreciates the analysis performed by GAO in this audit, GAO takes a security control specific approach to OPM's cybersecurity. However, GAO does not fully acknowledge OPM's "defense in depth" strategy and compensating controls. OPM has applied a "defense in depth" strategy to efforts to enhance OPM's cybersecurity posture, meaning there are many layers and aspects to OPM's defensive strategy. This strategy is supported and defined in NIST 800-53. Even if a potential vulnerability existed within the OPM environment, mitigations have been implemented that would require multiple defensive techniques to fail before a successful attack could be established. Since GAO did not acknowledge OPM's compensating controls, but rather performed an assessment based on the potential individual vulnerabilities, the report paints an incomplete, and ultimately, not fully accurate, picture of OPM's cybersecurity posture.

RESPONSE TO GAO RECOMMENDATIONS

Recommendation 1: Update the POA&M to reflect expected completion dates for implementing the recommendations made by US-CERT.
Response: We concur. OPM will update the POA&M with the current status, including expected completion dates, of POA&Ms created for implementing the recommendations made by US-CERT.

Recommendation 2: Improve the timeliness of validating evidence associated with actions taken to address recommendations.
Response: We partially concur. OPM will review its management practices to support more timely closure of POA&Ms.

Recommendation 3: Update policy to reflect deployment of DHS threat indicators and specific 24-hour scanning requirement.
Response: We concur. OPM is in the process of updating security policies which will include current operational practices of the scanning requirement.

Recommendation 4: Develop and implement role-based training requirements for staff using CDM tools.
Response: We concur. OPM is in the process of defining role-based training requirements for its continuous monitoring program, to include tools that support the CDM program.

Recommendation 5: Provide detailed guidance on the quality assurance process that includes evaluating security control assessments.
Response: We concur. As reported to GAO in April and June 2017, on related recommendations from GAO-14-612 and GAO-16-501, OPM is currently developing additional standards for evaluating security controls testing and will incorporate these standards into oversight procedures of security assessments. The standards will be used to evaluate future control assessments.

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

Sincerely,

DAVID DEVRIES

Digitally signed by DAVID DEVRIES
DN: c=US, o=U.S. Government, ou=Office of Personnel Management, cn=DAVID DEVRIES, 0.9.2342.19200300.100.1.1=24001003349144
Date: 2017.07.21 17:52:59 -04'00'

David L. DeVries
Chief Information Officer

2

Appendix III: 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, West Coile and Jeffrey Knott (assistant directors); Justin Palk (analyst-in-charge); Corey Evans, Nancy Glover, David Plocher, Brandon Sanders, Michael Stevens, and Edward Varty made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

Text of Appendix II: Comments from the Office of Personnel Management

Page 1

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, OPM Information Security, GAO-17-614, Job Code Number 100559.

OPM appreciates GAO's recognition of our significant progress in several information security areas. OPM has taken steps to enhance its cybersecurity posture in multiple areas through: the addition of cybersecurity tools and security updates; staff and agency-wide training; hiring critical personnel; and collaboration with OPM's interagency partners. OPM recognizes that cybersecurity is not just about technology, but is also about people. Therefore, in addition to strengthening technology, OPM has added seasoned cybersecurity and IT experts to an already talented team. OPM continues to leverage and utilize interagency partnerships and the expertise of the IT and cyber communities across government.

OPM welcomes and is receptive to the evaluation and feedback from GAO, as with other oversight entities, continuously drives to improve and enhance information security at OPM, and continues to implement changes that strengthen OPM's cybersecurity posture.

While OPM appreciates the analysis performed by GAO in this audit, GAO takes a security control specific approach to OPM's cybersecurity. However, GAO does not fully acknowledge OPM's "defense in depth" strategy and compensating controls. OPM has applied a "defense in depth" strategy to efforts to enhance OPM's cybersecurity posture, meaning there are many layers and aspects to OPM's defensive strategy. This strategy is supported and defined in NIST 800-53. Even if a potential vulnerability existed within the OPM environment, mitigations have been implemented that would require multiple defensive techniques to fail before a successful attack could be established. Since GAO did not acknowledge OPM's compensating controls, but rather performed an assessment based on the potential individual vulnerabilities, the report paints an incomplete, and ultimately, not fully accurate, picture of OPM's cybersecurity posture.

Page 2

RESPONSE TO GAO RECOMMENDATIONS

1. Recommendation 1: Update the POA&M to reflect expected completion dates for implementing the recommendations made by US-CERT.

Response: We concur. OPM will update the POA&M with the current status, including expected completion dates, of POA&Ms created for implementing the recommendations made by US-CERT.

2. Recommendation 2: Improve the timeliness of validating evidence associated with actions taken to address recommendations.

Response: We partially concur. OPM will review its management practices to support more timely closure of POA&Ms.

3. Recommendation 3: Update policy to reflect deployment of DHS threat indicators and specific 24-hour scanning requirement.

Response: We concur. OPM is in the process of updating security policies which will include current operational practices of the scanning requirement.

4. Recommendation 4: Develop and implement role-based training requirements for staff using CDM tools.

Response: We concur. OPM is in the process of defining role-based training requirements for its continuous monitoring program, to include tools that support the CDM program.

5. Recommendation 5: Provide detailed guidance on the quality assurance process that includes evaluating security control assessments.

Response: We concur. As reported to GAO in April and June 2017, on related recommendations from GAO-14-612 and GAO-16-501, OPM is currently developing additional standards for evaluating security controls testing and will incorporate these standards into oversight procedures of security assessments. The standards will be used to evaluate future control assessments.

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

Sincerely,

DAVID DEVRIES

Date: 2017.07.21 17:52:59 -04'00'

David L. DeVries

Chief Information Officer

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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