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

Accessible Version

November 13, 2018

The Honorable James Lankford
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
United States House of Representatives

**Information Security: OPM Has Implemented Many of GAO's 80 Recommendations, but Over One-Third Remain Open**

The Office of Personnel Management (OPM) collects and maintains personal data on millions of individuals, including data related to security clearance investigations. In June 2015, OPM reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate but related incident had compromised its systems and the files related to background investigations for 21.5 million individuals.

From February 2015 through August 2017, we conducted multiple reviews of OPM's information security. We issued four reports based on these reviews.[1] The reports contained 80 recommendations for improving the agency's security posture.

The Explanatory Statement that accompanies the *Consolidated Appropriations Act, 2018*, included a provision for GAO to brief the House and Senate Appropriations Committees on actions taken by OPM in response to GAO's information security recommendations.[2] Our

[1]GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016); *Information Security: OPM Needs to Improve Controls over Selected High-Impact Systems*, GAO-16-687SU (Washington, D.C.: Aug. 15, 2016); *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, GAO-17-459SU (Washington, D.C.: Aug. 3, 2017); and *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, GAO-17-614 (Washington, D.C.: Aug. 3, 2017).

[2]Explanatory Statement accompanying Pub. L. No. 115-141, Div. E, Title V (2018), 164 Cong. Rec. H2045, H2522 (March 22, 2018).

specific objective was to determine the extent to which OPM has implemented our recommendations to improve the agency's information security.

To accomplish this objective, we reviewed relevant documents and artifacts reflecting OPM's actions and progress toward implementing the 80 recommendations contained in the four reports, and assessed the actions against the intent of the recommendations. Our review examined the agency's actions taken on our recommendations through September 20, 2018. We also evaluated the agency's remedial action plans for those recommendations not yet implemented to determine the agency's intentions regarding the outstanding recommendations. Further, we interviewed officials in OPM's Office of the Chief Information Officer to obtain additional clarification about the agency's actions, as needed.

On September 26, 2018, we briefed members of your staff on the results of our review. This report formally transmits the final briefing slides (see enc. I).

We conducted this performance audit from September 2018 through November 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In summary, OPM has made progress in implementing our recommendations for improving its security posture, but further actions are needed. As of September 20, 2018, the agency had implemented 51 (about 64 percent) of the 80 recommendations, but had not provided any evidence, or provided insufficient evidence, to demonstrate implementation of the remaining recommendations, as shown in table 1.

**Table 1: OPM's Implementation of GAO's Information Security Program and Control Recommendations, as of September 20, 2018**

| n/a | Number of Recommendations | | | |
|---|---|---|---|---|
| **GAO Report Number** | **Closed–implemented** | **Open–insufficient evidence** | **Open–no evidence** | **Total** |
| GAO-16-501 | 0 | 1 | 3 | **4** |
| GAO-16-687SU | 46 | 2 | 14 | **62** |
| GAO-17-459SU | 2 | 1 | 6 | **9** |
| GAO-17-614 | 3 | 1 | 1 | **5** |
| **Total** | **51** | **5** | **24** | **80** |

Source: GAO analysis of OPM evidence. I GAO-19-143R

Notes: Closed-implemented: GAO validated that OPM implemented the recommendation.
Open-insufficient evidence: GAO determined that evidence provided by OPM was insufficient to demonstrate that the agency had implemented the recommendation.
Open-no evidence: OPM did not provide GAO with any evidence that the agency had implemented the recommendation.

The following provides further detail on the status of the recommendations, as of September 20, 2018, for each of the four reports:

- GAO-16-501 - OPM had not provided sufficient evidence to demonstrate that it had implemented the 4 recommendations. Three of the recommendations were related to enhancing security plans, performing comprehensive security control assessments, and

updating remedial action plans for two selected high-impact systems.[3] The fourth recommendation was to provide and track specialized training for all individuals, including contractors, who have significant security responsibilities. We designated 3 of the 4 recommendations as priority recommendations.[4]

- GAO-16-687SU – Of the 62 recommendations GAO made in this report, OPM had implemented or addressed 46 recommendations,[5] including those recommendations associated with strengthening firewall controls, enforcing password policies, restricting access to a key server, logging security-related activities, and updating the contingency plan for a high-impact system. However, the agency had not provided sufficient evidence that it had implemented the other 16 recommendations. These recommendations included avoiding the use of the same administrator accounts by multiple persons, implementing procedures governing the use of special privileges on a key computer, encrypting passwords while stored or in-transit across the network, and installing the latest versions of operating system software on network devices supporting a high-impact system.
- GAO-17-459SU – OPM had implemented 2 of the 9 recommendations we made in this report. In response to the 2 recommendations, the agency improved its protection of data by encrypting data for two selected systems we reviewed. However, the agency had not demonstrated that it had fully implemented 7 other recommendations, including recommendations to reset all passwords subsequent to the breach, install critical patches in a timely manner, periodically evaluate accounts to ensure privileged access is warranted, and assess controls on selected systems as defined in its continuous monitoring plan.
- GAO-17-614 - OPM had implemented 3 of the 5 recommendations in this report. The agency had updated milestones for completing United States Computer Emergency Readiness Team recommendations[6] and its policy for deploying threat indicators, and had improved its guidance for evaluating the quality of control assessments. However, the agency had not demonstrated that it had implemented 2 recommendations that we had designated as priority recommendations[7] to improve the timeliness of validating corrective actions and to develop and implement training requirements for staff using special tools.

[3]Systems that agencies categorize as high impact are those systems where the loss of confidentiality, integrity, or availability could have a severe or catastrophic adverse effect on organizational operations, assets, or individuals.

[4]Priority recommendations are those that GAO believes warrant priority attention from heads of departments and agencies. In a July 2016 letter to OPM's Acting Director, the Comptroller General informed her of these three priority recommendations related to strengthening controls for high-impact systems. In June 2017, the Comptroller General sent a similar letter highlighting these three priority recommendations to another OPM Acting Director, as well as in another letter to the OPM Director in March 2018 because the agency had not implemented the recommendations.

[5]OPM addressed 21 of the 46 recommendations through the decommissioning of one of the two high-impact systems that we reviewed.

[6]The United States Computer Emergency Readiness Team (US-CERT), a component of the Department of Homeland Security, operates the federal information security incident center. In September 2015, US-CERT made 19 recommendations to OPM to bolster the agency's information security practices and controls in the wake of the 2015 breaches.

[7]Based on the need to strengthen controls over information technology systems, in a March 2018 letter to the OPM Director, the Comptroller General cited these two additional priority recommendations from our August 2017 report.

According to officials in OPM's Office of the Chief Information Officer, the agency plans to implement 25 of the remaining 29 open recommendations by the end of calendar year 2018. The agency expects to implement 3 additional recommendations by the end of fiscal year 2019. OPM has created remedial action plans for each of the 28 open recommendations that it plans to implement.

However, the officials stated that the agency does not plan to implement the one remaining recommendation related to deploying a security tool on contractor workstations. The agency asserted that it has compensating controls in place to address the intent of this recommendation, but has not provided evidence to us of these controls. Expeditiously implementing all remaining open recommendations is essential to ensuring that appropriate controls are in place to protect the agency's systems and information.

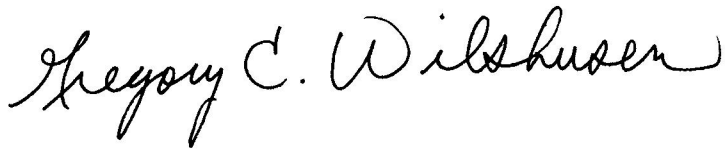
**Agency Comments**

We provided a draft of this report to the Acting Director of the Office of Personnel Management. The agency had no additional comments beyond what is reprinted in the enclosed briefing slides.

---

We are sending copies of this report to the appropriate congressional committees, the Acting Director of OPM, the OPM 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.

If you or your staff members have any questions concerning this report, please contact me at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Jeffrey Knott (assistant director), Nancy Glover, Vernetta Marquis, Mary Marshall, Kevin Metcalfe, and Michael Stevens.



Gregory C. Wilshusen
Director, Information Security Issues

Enclosure

(103011)

GAO

# OPM Has Implemented Many of GAO's 80 Information Security Recommendations, but Over One Third Remain Open

## A Briefing for Staff of the Senate and House Appropriations Subcommittees on Financial Services and General Government

## September 26, 2018

For more information, contact Gregory C. Wilshusen at wilshuseng@gao.gov or (202) 512-6244.

# Contents

# Background

- The Office of Personnel Management (OPM) collects and maintains personal data on millions of individuals, including data related to security clearance investigations.
- In June 2015, OPM reported that an intrusion into its information systems had compromised 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 data files related to background investigations for 21.5 million individuals.

# Background (cont.)

The *Federal Information Security Modernization Act of 2014* requires agencies to implement an information security program that includes, among other things,

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- plans for providing adequate information security for networks and systems;
- training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices; and
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, or practices of the agency.

# Background (cont.)

Governmentwide information security requirements include, among other things:

- tightening policies and practices for privileged users by inventorying and minimizing the number of privileged users,
- when the assessed risk indicates the need, encrypting federal information at rest and in transit unless otherwise protected by alternative physical and logical safeguards, and
- developing and maintaining a strategy for monitoring information security controls on an ongoing and continuous basis.

# Background (cont.)

- From February 2015 through August 2017, we conducted multiple reviews of OPM's information security. We issued four reports based on these reviews. The reports contained 80 recommendations for improving the agency's information security posture.
- The Explanatory Statement that accompanies the *Consolidated Appropriations Act, 2018,* included a provision for GAO to brief the House and Senate Appropriations Subcommittees on Financial Services and General Government on actions taken by OPM in response to GAO's information security recommendations.[1]

[1]Explanatory Statement to accompany Pub. L. No. 115-141, Div. E, Title V (2018), 164 Cong. Rec. H2045, H2522 (March 22, 2018).

# Objective

Our objective was to:

- Determine the extent to which OPM has implemented GAO's recommendations to improve the agency's information security.

# Scope and Methodology

We examined OPM's implementation of the 80 recommendations contained in the following four reports:

1. *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501, May 18, 2016.
2. *Information Security: OPM Needs to Improve Controls over Selected High-Impact Systems*, GAO-16-687SU, August 15, 2016.
3. *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, GAO-17-459SU, August 3, 2017.
4. *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed*, GAO-17-614, August 3, 2017 (public version of GAO-17-459SU).

We considered the corrective actions that OPM had taken as of September 20, 2018.

# Scope and Methodology (cont.)

To accomplish the objective, we:

- reviewed relevant documents and artifacts reflecting OPM's actions and progress toward implementing our recommendations, and assessed the agency's actions against the intent of the recommendations;
- evaluated the agency's remedial action plans for recommendations not yet implemented to determine the agency's intentions regarding these recommendations; and
- interviewed officials in OPM's Office of the Chief Information Officer to obtain clarification on the actions taken to implement the recommendations, as needed.

# Scope and Methodology (cont.)

We conducted this performance audit in September 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

# Results in Brief

- OPM has made progress in implementing GAO's information security recommendations, but further efforts remain. As of September 20, 2018, the agency had implemented 51 of the 80 recommendations.
- For the 29 open recommendations, OPM has not provided any evidence, or insufficient evidence, to demonstrate implementation.
- OPM intends to implement 25 of the 29 open recommendations by the end of 2018 and 3 of them by the end of fiscal year 2019. The agency does not intend to implement one of the recommendations to deploy a security tool on contractor workstations. OPM stated it had compensating controls, but has not provided evidence of them.
- Expeditiously implementing the open recommendations is essential to ensuring appropriate controls are in place to protect the agency's systems and information.

# Prior Findings and Current Status of Recommendations

As of September 20, 2018, OPM had implemented many recommendations; nonetheless, over one-third remain open because the agency has not yet provided any evidence, or has provided insufficient evidence, to demonstrate that it has taken the actions we recommended. See table 1.

Table 1: OPM's implementation of GAO's information security program and control recommendations, as of September 20, 2018.

| n/a | Number of Recommendations | | | |
|---|---|---|---|---|
| GAO Report | Closed - implemented | Open – insufficient evidence provided | Open – no evidence provided | Total |
| GAO-16-501 | 0 | 1 | 3 | 4 |
| GAO-16-687SU | 46 | 2 | 14 | 62 |
| GAO-17-459SU | 2 | 1 | 6 | 9 |
| GAO-17-614 | 3 | 1 | 1 | 5 |
| Totals | 51 | 5 | 24 | 80 |

Source: GAO analysis of OPM evidence.

# Prior Findings and Current Status of Recommendations – GAO-16-501

In a May 2016 report on federal agencies' implementation of controls over their high-impact systems,[2] we noted that weaknesses existed in the two OPM high-impact information systems that we reviewed. These weaknesses existed, in part, because OPM had not effectively implemented elements of its information security program.

Although the agency had developed risk assessments for the two selected systems and a continuous monitoring strategy that included performance metrics, it had not taken other steps.

[2]Systems that agencies categorize as high impact are those systems where the loss of confidentiality, integrity, or availability can have a severe or catastrophic adverse effect on organizational operations, assets, or individuals.

# Prior Findings and Current Status of Recommendations - GAO-16-501 (cont.)

For example:

- Although OPM had identified almost all controls required for high-impact systems in the security plan for one of the selected systems, the agency had identified only about half of the high-impact controls in the other system's plan.
- OPM also had not performed comprehensive security control assessments. For example, in performing its assessments, OPM had not identified the access control weaknesses that we identified during our review.
- The agency had not included updated milestones in its remedial action plans.
- The agency was not tracking specialized training for all individuals with significant security responsibilities.

# Prior Findings and Current Status of Recommendations - GAO-16-501 (cont.)

- We made 4 recommendations, including 3 priority recommendations,[3] to enhance security plans, perform comprehensive security control assessments, and update remedial action plans for selected systems, and track specialized training.
- OPM concurred with 2 of the 4 recommendations (security and remedial action plans), partially concurred with a third (specialized training), and did not concur with a fourth recommendation (security control assessments). OPM subsequently developed remedial action plans to implement all 4 recommendations.
- As of September 20, 2018, OPM had not provided sufficient evidence to demonstrate that it had implemented any of the 4 recommendations.

[3]Priority recommendations are those that GAO believes warrant priority attention from heads of departments and agencies.

# Prior Findings and Current Status of Recommendations – GAO-16-687SU

In an August 2016 report, we noted that the agency had established controls for the two high-impact systems we reviewed. However, we pointed out that OPM had not always effectively implemented these controls in a manner to protect the confidentiality, integrity, and availability of the systems. Specifically, the agency had not adequately controlled access to the systems.

# Prior Findings and Current Status of Recommendations - GAO-16-687SU (cont.)

For example, OPM had not always:

- protected the selected systems' boundaries[4]
- enforced password policies for authenticating access to the systems
- restricted access to only that needed to perform job duties
- enabled encryption for a database
- provided sufficient logging for auditing and monitoring the systems.

Weaknesses also existed in configuration management and contingency planning for the two selected systems.

[4] Boundary protection controls pertain to the protection of a logical boundary around a system by implementing measures to prevent unauthorized information exchange across the boundary in either direction.

# Prior Findings and Current Status of Recommendations - GAO-16-687SU (cont.)

- We made 62 recommendations to OPM to mitigate weaknesses that we identified in access controls, configuration management, and contingency planning for the two systems.
- OPM concurred with the recommendations for one of the two systems. At the time that we issued our report, the agency stated that the other system, which was contractor-operated, had been disconnected, and that the agency would evaluate the recommendations for that system when a new contract was in place.
- Subsequently, in December 2016, OPM stated that it had contracted with a vendor, and that the vendor was actively working to address our recommendations for the second system.

# Prior Findings and Current Status of Recommendations - GAO-16-687SU (cont.)

As of September 20, 2018, OPM had implemented or addressed[5] forty-six of the sixty-two recommendations, including those recommendations associated with:

- strengthening firewall controls
- enforcing password policies
- restricting access to a key server
- logging security-related activities
- updating the contingency plan for a high-impact system.

[5]OPM addressed 21 of the 46 recommendations through the decommissioning of one of the two high-impact systems that we reviewed.

# Prior Findings and Current Status of Recommendations - GAO-16-687SU (cont.)

However, OPM had not provided sufficient evidence that it had implemented the other 16 recommendations. These recommendations included:

- avoiding the use of the same administrator accounts by multiple people;
- implementing procedures governing the use of special privileges on a key computer;
- encrypting passwords while stored or in-transit across the network; and
- installing the latest versions of operating system software on network devices supporting a high-impact system.

OPM had developed remedial action plans for each of the 16 open recommendations.

# Prior Findings and Current Status of Recommendations – GAO-17-459SU

In an August 2017 report on OPM's efforts to improve its security program, we noted that the agency had implemented or made progress toward implementing 19 recommendations that the United States Computer Emergency Readiness Team (US-CERT)[6] had previously made to bolster OPM's information security practices and controls in the wake of the 2015 breaches.

Specifically, OPM had implemented 11 of the US-CERT recommendations and had partially implemented the remaining 8 recommendations, with actions for 4 of the 8 requiring further improvement.

[6] The United States Computer Emergency Readiness Team, a component of DHS, operates the federal information security incident center.

# Prior Findings and Current Status of Recommendations - GAO-17-459SU (cont.)

- We reported that OPM had also made progress in implementing information security policies and practices associated with certain government-wide requirements. However, it had not fully implemented all of the requirements.
- We made 9 recommendations for OPM to improve upon the actions it had taken to implement the US-CERT recommendations and to further implement government-wide requirements.

# Prior Findings and Current Status of Recommendations - GAO-17-459SU (cont.)

- OPM concurred with 7 of our recommendations, partially concurred with 1 recommendation, and had developed remedial action plans to implement all 8 of these recommendations.
- The agency did not concur with, and does not plan to implement, our recommendation related to deploying a security tool on contractor workstations. OPM asserted that it had compensating controls in place, but has not yet provided sufficient evidence of these controls.

# Prior Findings and Current Status of Recommendations - GAO-17-459SU (cont.)

As of September 20, 2018, OPM had improved its protection of data by implementing 2 of our recommendations related to encrypting data for two of the selected systems that we reviewed.

However, the agency had not demonstrated that it had fully implemented the other 6 recommendations for which it concurred or partially concurred, including recommendations to

- reset all passwords subsequent to the breach;
- install critical patches in a timely manner;
- periodically evaluate accounts to ensure privileged access is warranted; and
- assess controls on selected systems as defined in its continuous monitoring plan.

# Prior Findings and Current Status of Recommendations – GAO-17-614

In our fourth report, issued in August 2017, we noted that, although OPM had made progress toward implementing the US-CERT recommendations and addressing government-wide requirements, the agency had not

- validated remedial actions related to the recommendations in a timely manner or consistently updated milestones for outstanding recommendations;
- complied with its own plan for conducting periodic control assessments;
- documented role-based training requirements for individuals configuring and maintaining monitoring tools; and
- always comprehensively tested key security controls on selected contractor-operated systems.

# Prior Findings and Current Status of Recommendations - GAO-17-614 (cont.)

We made 5 recommendations, including 2 priority recommendations, for OPM to further improve its security posture. These recommendations were related to

- updating milestones for completing the US-CERT recommendations,
- validating remedial actions more timely,
- updating policy for deploying threat indicators,
- developing and implementing training requirements for staff using monitoring tools, and
- providing guidance on evaluating the quality of control assessments.

# Prior Findings and Current Status of Recommendations - GAO-17-614 (cont.)

- OPM concurred with 4 of the 5 recommendations, partially concurred with 1 recommendation, and had developed remedial action plans to implement all 5 recommendations.
- As of September 20, 2018, OPM had implemented 3 of the recommendations. Specifically, the agency had updated (1) milestones for completing US-CERT recommendations and (2) its policy for deploying threat indicators. The agency had also improved its guidance for evaluating the quality of control assessments.
- However, the agency could not demonstrate that it had implemented the 2 priority recommendations to improve the timeliness of validating corrective actions, and to develop and implement training requirements for staff using monitoring tools.

# Prior Findings and Current Status of Recommendations

- According to officials in OPM's Office of the Chief Information Officer, OPM plans to implement 25 of the remaining 29 open recommendations by the end of 2018. The agency expects to implement 3 recommendations by the end of fiscal year 2019.
- As previously noted, OPM does not plan to implement the 1 remaining recommendation to install a security tool on contractor workstations.

# GAO Summary

- Implementing all of  the remaining open recommendations expeditiously is essential to OPM ensuring that appropriate security controls are in place and operating as intended.
- Until OPM implements these recommendations, its systems and information will be at increased risk of unauthorized access, use, disclosure, modification, or disruption.

# Agency Comments

In providing written comments on a draft of these slides, OPM stated the following:

- During FY 2018, OPM made significant progress addressing GAO recommendations.
- In FY 2018, the agency committed significant resources to address GAO audit recommendations.
- This commitment has resulted in noteworthy progress, demonstrated by the implementation of 51 of the recommendations in FY 2018 alone.
- OPM is dedicated to continued implementation of the remaining recommendations, projecting implementation of 5 more recommendations during this final quarter of FY18.
- OPM will build on the progress of FY 2018 with planned implementation of 20 recommendations in Q1 of FY 2019 and the remaining 3 recommendations in Q4 of FY 2019.

# Agency Comments (cont.)

OPM also provided the graph below regarding the number of GAO information security recommendations implemented by quarter in fiscal year 2018: