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.