GAO Highlights

Highlights of GAO-20-199, a report to congressional committees

February 2020

OFFICE OF CONGRESSIONAL WORKPLACE RIGHTS

Weaknesses in Cybersecurity Management and Oversight Need to Be Addressed

Why GAO Did This Study

OCWR is an independent, nonpartisan office that administers and enforces various provisions related to fair employment, and occupational safety and health within the legislative branch. To meet its mission, OCWR relies extensively on external parties, such as the Library of Congress, for IT support. In December 2018, Congress passed the Congressional Accountability Act of 1995 Reform Act (Reform Act) which, among other things, required OCWR to create a secure, online system to receive and keep track of claims related to employee rights and protections, such as sexual harassment and discrimination. To meet this requirement, OCWR initiated the SOCRATES project to upgrade its legacy claims management system.

The Reform Act included a provision for GAO to review OCWR's cybersecurity practices. This report examines the extent to which OCWR (1) incorporated key cybersecurity management activities into project planning for its claims management system upgrade, (2) performed oversight of security controls and mitigated risks for selected systems operated by external parties on its behalf and, (3) established an effective approach for managing organization-wide cybersecurity risk. To address these objectives, GAO compared OCWR IT policies, procedures, strategic plans, and documentation for two selected systems to leading IT project planning, system oversight, and cybersecurity management practices.

What GAO Recommends

GAO is making five recommendations to OCWR to address weaknesses in cybersecurity management and oversight. OCWR did not state whether it agreed or disagreed with GAO's recommendations, but described actions planned or taken to address them.

View GAO-20-199. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The Office of Congressional Workplace Rights (OCWR) did not incorporate key cybersecurity management practices into the planning for its Secure Online Claims Reporting and Tracking E-filing System (SOCRATES) project. While OCWR drafted a SOCRATES project schedule, the office did not finalize and use this schedule to manage cybersecurity activities, such as the time frames for conducting information technology (IT) system security assessments. In addition, the office did not document project cybersecurity risks, such as the office's reliance on external parties to implement responsibilities on its behalf. These weaknesses were due, in part, to a lack of policies and procedures for IT project planning. Until OCWR establishes and implements such policies and procedures, it will continue to have a limited ability to effectively manage and monitor the completion of cybersecurity activities for its IT projects.

OCWR did not fully implement important oversight activities for two selected systems—SOCRATES and the system used to document occupational safety and health violations known as the Facility Management Assistant (FMA)—operated by external entities (see table).

Extent to Which the Office of Congressional Workplace Rights (OCWR) Implemented Selected System Oversight Activities for Two Systems Operated by External Entities

	Establish security and privacy requirements	Plan assessment of security controls	Conduct assessment	Review assessment
Secure Online Claims Reporting and Tracking E-filing System (SOCRATES)	◐	◐	◐	◐
Facility Management Assistant (FMA)	◐	○	○	○

Key: ● Fully implemented ◐ Partially implemented ○ Not implemented

Source: GAO analysis of agency and external contractor data. | GAO-20-199

These shortfalls contributed to concerns with the deployment of SOCRATES in June 2019. For example, important security controls needed to ensure the confidentiality, integrity, and availability of the system were not fully tested before the system was deployed. In addition, penetration testing—where evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of the system—was not fully completed before deployment. GAO plans to issue a separate report with limited distribution on its assessment of security controls intended to, among other things, prevent successful attacks.

Although OCWR's strategic plan includes a goal of developing cybersecurity policies and procedures, the office had not fully established an effective approach for managing organization-wide cybersecurity risk. For example, OCWR designated an executive to oversee risk, but had not established the responsibilities of the official in the office's policies. Until OCWR improves its appoach to managing cybersecurity risks, its ability to make operational decisions that adequately address security risks will be hindered.