United States Government Accountability Office

Report to Congressional Committees

February 2020

OFFICE OF CONGRESSIONAL WORKPLACE RIGHTS

Weaknesses in Cybersecurity Management and Oversight Need to Be Addressed

GAO-20-199

February 2020

OFFICE OF CONGRESSIONAL WORKPLACE RIGHTS

Weaknesses in Cybersecurity Management and Oversight Need to Be Addressed

GAO Highlights

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

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.

Contents

Abbreviations

CAA	Congressional Accountability Act of 1995
CMMI-ACQ	Capability Maturity Model Integration® for Acquisition
CMMI-DEV	Capability Maturity Model Integration® for Development
CMS	Case Management System
FISMA	Federal Information Security Modernization Act of 2014
FMA	Facility Management Assistant
IT	information technology
Library	Library of Congress
NIST	National Institute of Standards and Technology
OCWR	Office of Congressional Workplace Rights
POA&M	plan of action and milestones
SOCRATES	Secure Online Claims Reporting and Tracking E-filing System
SP	special publication

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

February 11, 2020

The Honorable Roy Blunt
Chairman
The Honorable Amy Klobuchar
Ranking Member
Committee on Rules and Administration
United States Senate

The Honorable Zoe Lofgren
Chairman
The Honorable Rodney Davis
Ranking Member
Committee on House Administration
House of Representatives

The Congressional Accountability Act of 1995 (CAA) established the Office of Congressional Workplace Rights (OCWR), formerly the Office of Compliance, to administer and enforce various provisions related to fair employment, and occupational safety and health within the legislative branch.[1] OCWR is an independent, nonpartisan office and its work covers approximately 30,000 legislative branch employees in the Washington, D.C., area, as well as elected officials' district and state offices.[2]

The CAA of 1995 Reform Act (Reform Act), enacted on December 21, 2018, amended the procedures for initiating, conducting the preliminary review, and resolving claims related to violations of employee rights and protections, such as sexual harassment or discrimination.[3] Among other things, the Reform Act required OCWR to establish an electronic system

[1]Pub. L. No. 104-1, 2 U.S.C. §§ 1301-1438.

[2]Generally, the CAA applies to the following employers and their employees: House of Representatives, Senate, the Capitol Police, the Congressional Budget Office, the Office of the Architect of the Capitol (including the Office of Congressional Accessibility Services), the Office of the Attending Physician, the Office of Congressional Workplace Rights, the Office of Technology Assessment (not currently staffed), the Library of Congress (except for section 1351), the John C. Stennis Center for Public Service Training and Development, the China Review Commission, the Congressional-Executive China Commission, and the Helsinki Commission. Certain provisions of the CAA also apply to us and our employees.

[3]Pub. L. No. 115-397, 132 Stat. 5297 (Dec. 21, 2018).

to receive and keep track of claims by June 19, 2019. In response, OCWR initiated the Secure Online Claims Reporting and Tracking E-filing System (SOCRATES) project, which is intended to fulfill the Reform Act's requirement of establishing an electronic system for claims. According to OCWR officials, this project is intended to be an upgrade to OCWR's legacy claims management system.

To carry out its required functions, OCWR relies on two external parties—the Library of Congress (Library) and an external contractor—for information technology (IT) services and systems support, including assistance with upgrading its legacy claim management system to SOCRATES. The external contractor also provides hosting and application support for another system—the Facility Management Assistant (FMA)—which is a record-keeping system OCWR uses to document occupational safety and health violations.

Because OCWR is dependent on IT systems to collect and maintain sensitive data, such as the claims of legislative branch employees that their rights and protections have allegedly been violated, the security of these systems and data is vital to public confidence. These systems contain a vast amount of sensitive and personally identifiable information,[4] thus making it imperative to protect the confidentiality, integrity, and availability of this information.

The risks to IT systems supporting the federal government are increasing as security threats continue to evolve and become more sophisticated. These risks include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks. Underscoring the importance of this issue, we continue to designate information security as a government-wide high-risk

[4]Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

area in our most recent biennial report to Congress—a designation we have made in each report since 1997.[5]

In light of the importance of cybersecurity to federal IT systems, the Reform Act included a provision for us to review OCWR's cybersecurity practices. This report examines the extent to which OCWR (1) incorporated key cybersecurity management activities into the 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 organization-wide approach for managing cybersecurity risk.

To determine the extent to which OCWR has incorporated key cybersecurity management activities into its SOCRATES project planning, we reviewed available OCWR project planning documentation related to establishing a project schedule, a requirements management process, and a risk management process. We then compared the office's available project planning documentation to leading practices for project planning, including those identified by the Software Engineering Institute.[6]

We also analyzed the documentation to determine the extent to which OCWR incorporated key cybersecurity management activities, as identified by the National Institute of Standards and Technology (NIST) risk management framework.[7] These activities include, for example, selecting and implementing information security controls and assessing the security controls. Finally, we interviewed OCWR officials, including the General Counsel and the Director of the IT Governance, Risk Management, and InfoSec Compliance Program.

[5]See *GAO, High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: March 2019) and *High Risk Series: An Overview*, GAO/HR-97-1 (Washington, D.C.: February 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[6]The Software Engineering Institute at Carnegie Mellon University is a Federally Funded Research and Development Center —a nonprofit, public–private partnership that conducts research for the U.S. government. It conducts research and development in software engineering, systems engineering, cybersecurity, and many other areas of computing, working to introduce private-sector innovations into government.

[7]NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* Special Publication (SP) 800-37, Revision (Rev.) 2 (Gaithersburg, Md.: December 2018).

To determine the extent to which OCWR performed oversight of security controls and mitigated risks for the two selected systems operated by external parties on its behalf, SOCRATES and FMA, we collected and reviewed OCWR's cybersecurity policies, procedures, and documentation (e.g., system security plans) related to the office's two systems and external partners. The external partners were the Library and OCWR's external contractor. We chose these two systems because they process and maintain OCWR's most sensitive information,[8] including claims related to alleged violations of employee rights and protections and reported occupational safety and health violations.[9]

We then examined whether OCWR and its external partners implemented—for each selected system—four oversight activities important for assessing the security and privacy controls of information systems operated by external entities, as specified in federal requirements and guidance, including NIST guidance.[10] The four oversight activities we examined were: (1) establishing security and privacy requirements, (2) planning the assessment of security controls, (3) conducting the assessment, and (4) reviewing the assessment. We chose these activities because of their importance to providing effective oversight of systems operated by external entities. We also conducted interviews with OCWR officials, including the General Counsel and Director of the IT Governance, Risk Management, and InfoSec Compliance Program. In addition, we interviewed personnel from OCWR's external partners, including the Library's Deputy Chief Information Officer.

To determine the extent to which OCWR established an effective organization-wide approach for managing cybersecurity risk, we obtained and reviewed available documentation related to OCWR's information security policies and procedures, management reports, and strategic planning. We then assessed whether the office's approach for managing

[8]OCWR also uses a third externally-operated system for, among other things, accessing information related to the Americans with Disabilities Act of 1990 (e.g., accessibility standards). According to OCWR's General Counsel, this system contains information reproduced in publicly available reports.

[9]Reported occupational safety and health violations may contain sensitive information related to vulnerabilities in legislative branch facilities (e.g., fire safety) that could be exploited to exacerbate the harm caused by a physical attack.

[10]See NIST, *Guide to Information Technology Services*, SP 800-35 (Gaithersburg, Md.: October 2003) and NIST SP 800-37, Rev. 2.

organization-wide cybersecurity risk addressed foundational cybersecurity risk management components identified in NIST guidance, including NIST's risk management framework.[11] These components were the establishment of a risk executive function, cybersecurity risk management strategy, and risk-based security policies and procedures.

We also interviewed OCWR officials, including the General Counsel and Director of the IT Governance, Risk Management, and InfoSec Compliance Program, regarding their efforts to establish an approach for managing cybersecurity risk. See appendix I for a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from January 2019 to February 2020 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

Enacted on January 23, 1995, the CAA, as amended, applies 13 federal civil rights, workplace, and labor laws to legislative branch employees who were previously exempted from such coverage.[12] Table 1 lists the 13 laws included under the CAA.

Table 1: The 13 Civil Rights, Workplace, and Labor Laws Included under the Congressional Accountability Act (CAA) As Amended

CAA-covered federal law	Summary of provisions
1. Title VII of the Civil Rights Act of 1964, as amended	Prohibits discrimination in hiring, promotion, and treatment of employees based on race, sex, color, religion, or national origin.
2. The Age Discrimination in Employment Act of 1967, as amended	Prohibits discrimination in hiring, promotion, and treatment of employees based on age.
3. The Rehabilitation Act of 1973	A precursor to the Americans with Disabilities Act; prohibits discrimination against qualified individuals with disabilities with regard to federal employment.
4. The Family and Medical Leave Act of 1993	Provides that employees may use unpaid leave for certain family and medical needs.

[11]NIST, SP 800-37, Rev. 2.

[12]Pub. L. No. 104-1, 2 U.S.C. §§ 1301-1438.

CAA-covered federal law	Summary of provisions
5. The Fair Labor Standards Act of 1938, as amended	Provides for fair compensation for employees for work performed.
6. The Employee Polygraph Protection Act of 1988	Prohibits most private employers from requiring employees and prospective employees to take a polygraph examination.
7. The Worker Adjustment and Retraining Notification Act	Requires employers to provide advance notice of plant closings and mass layoffs.
8. Chapter 43 of title 38 of the U.S. Code (relating to veterans' employment and reemployment)	Provides reemployment rights for employees who serve in the uniformed services.
9. The Americans with Disabilities Act of 1990	Prohibits discrimination in hiring, promotions, and treatment of employees on the basis of disability; requires full and equal access to public accommodations for the disabled.
10. The Occupational Safety and Health Act of 1970	Requires employers to provide a workplace that complies with occupational safety and health standards.
11. Chapter 71 of title 5 U.S.C. (relating to federal labor management relations)	Protects the rights and obligations of employers and employees in labor-management relations.
12. Veterans' Employment Opportunities Act of 1998	Provides hiring preferences for veterans.
13. Genetic Information Nondiscrimination Act of 2008	Protects employees from employment discrimination and denial of health insurance based on their genetic information.

Source: GAO based on the CAA, as amended. | GAO-20-199

The CAA contained a series of specific requirements for the Office of Compliance to meet as it carried out its responsibility to administer and enforce the act. Toward this end, the Office of Compliance took a number of actions, such as administering a dispute resolution process;[13] conducting investigations and inspections to ensure compliance with safety, health, and disability access standards; investigating and managing matters concerning labor management relations, and educating both employees and employing offices about their rights and responsibilities under the CAA.

The Reform Act expanded the office's duties and responsibilities, as well as the number of employees covered by the CAA. These new duties and responsibilities include, among other things:

- changing the name of the office to OCWR;
- substantially modifying the administrative dispute resolution process under the CAA, including creating additional procedures for preliminary hearing officer review of claims;

[13]OCWR manages an administrative dispute resolution process to resolve alleged violations of workplace rights and protections, such as discrimination.

- appointing one or more advisers to provide confidential information to legislative branch employees about their rights under the CAA;
- extending CAA protections to unpaid staff, including interns, detailees, and fellows, as well as previously unprotected legislative branch employees;
- conducting a workplace climate survey;
- significantly expanding OCWR reporting obligations;
- creating a program to permanently retain records of investigations, mediations, hearings, and other proceedings; and
- establishing an electronic system to receive and keep track of claims.

The act mandated that OCWR institute some of these requirements, such as changing the name of the office, immediately. Other requirements, such as establishing an electronic system to receive and keep track of claims, were to be met no later than 180 days after the implementation of the act, or by June 19, 2019.

To implement its statutory requirements, OCWR currently has 28 full-time equivalent positions, which includes five part-time members of OCWR's Board of Directors (counted as one full-time equivalent) appointed by congressional leadership. This represents an increase of five full-time equivalents since April 2018.

OCWR Relies on External Entities to Provide IT Services and Systems, Including the Upgrade to Its Claims Management System

OCWR relies extensively on IT services and systems provided by external parties to support its mission-related operations and protect claims data. For example, the Library provides network and end-user computing services for OCWR, including email; network services such as Internet access and file sharing; and end-user services and support, such as desktop support and software management.

OCWR also relied on an external contractor to develop and maintain its legacy claims management system, known as the Case Management System (CMS). Since 2014, the office used CMS to manage claims submitted by covered legislative branch employees using one of four ways: in person at OCWR's office; or by mail, email, or fax. After a claim was received, an OCWR employee would manually enter the claim information into CMS and update the information as it progressed through the dispute resolution process.

In response to the Reform Act enacted in December 2018, OCWR initiated the SOCRATES project to meet the requirement of implementing an electronic system for claims. SOCRATES is intended to enable covered legislative branch employees to file a claim via a web-based form, and an OCWR employee to electronically manage the workflow of claims as they progress through the dispute resolution process.[14] Specifically, the system is expected to maintain and track claim deadlines, generate correspondence, as well as update and store claim information.

OCWR relied on both the Library and an external contractor to upgrade CMS to SOCRATES. As part of its SOCRATES implementation efforts, OCWR first moved the CMS application and claim data from its office to the Library, which began hosting the system in April 2019.[15] Between April 2019 and June 2019, OCWR's external contractor continued work to develop and implement new and updated components for CMS to facilitate the electronic filing and management of claims. In addition, the external contractor worked to develop and implement the web-based form to electronically capture claims. According to OCWR, SOCRATES is comprised of three components that are hosted by the Library:

- **SOCRATES web-based form:** This form is intended to be used by covered legislative branch employees to submit a claim alleging a violation of civil rights, workplace, or labor laws during their employment.
- **Secure information sharing platform:**[16] This platform is intended to be a web-based, secure workflow file collaboration application. The platform allows for the sharing of claim related information between OCWR, the covered employee, the employee's office, and any other relevant parties (e.g., employee representatives).

[14]In addition to filing claims online by accessing the OCWR website and submitting their information using an electronic form, covered legislative branch employees still have the option to file a claim at OCWR's office, or by mail, email, or fax.

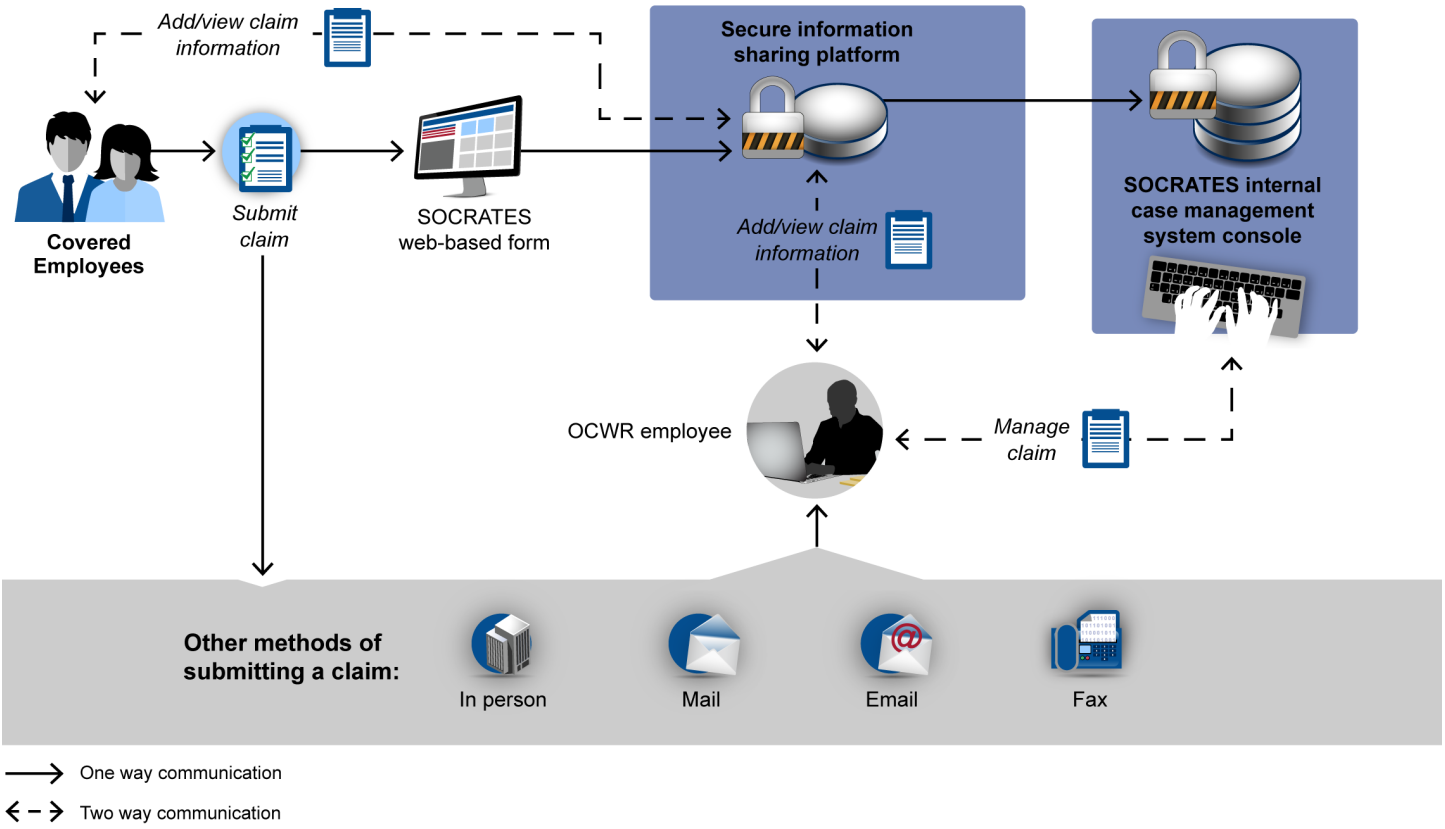
[15]OCWR transitioned CMS to the Library following Congressional concerns about adequate oversight and protection over a third party contractor storing sensitive nonpublic claim information.

[16]In May 2019, OCWR entered into an agreement with another external contractor to support the installation and maintenance of the secure information sharing platform within the Library's environment.

- **SOCRATES internal CMS console:** Based on updated functionality from OCWR's CMS, this console is intended to provide secure, detailed workflow management of each claim that is submitted. Specifically, the console introduces new workflows based on the Reform Act's updated requirements for a claim and allows OCWR employees to internally manage a claim.

Figure 1 shows the updated claim filing process using SOCRATES.

Figure 1: SOCRATES Claim Filing Process



SOCRATES (Secure Online Claims Reporting and Tracking E-filing System), OCWR (Office of Congressional Workplace Rights), Library (Library of Congress)

Source: GAO analysis of OCWR and Library documentation. | GAO-20-199

According to OCWR, testing of SOCRATES the week prior to its June 19, 2019, due date revealed numerous problems with the system. For example, if a user did not submit his or her claim within a certain amount of time, the system refreshed the webpage without saving the user's data, forcing the user to restart the claim. As a result, OCWR delayed the

deployment 7 days to allow time to resolve this issue and others. On June 26, 2019, OCWR deployed SOCRATES and began accepting claims via the web-based form.[17]

In addition to SOCRATES, OCWR relies on the external contractor to provide hosting and application support for FMA. FMA is used by OCWR to document reported violations of the Occupational Safety and Health Act. The CAA requires OCWR to conduct biennial inspections of the legislative branch to ascertain compliance with the act and to report its findings to Congress. The office also reports its findings to the legislative branch agency that is reportedly in violation of the act in a Hazard Summary Report. The agency is responsible for responding, and providing verification of the abatement of violations and hazards documented in the findings, to OCWR.

Federal Information and Systems Are Increasingly Targeted by Cybersecurity Threats

IT systems supporting federal agencies are inherently at risk. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks. Compounding the risk, federal systems and networks are also often interconnected with other internal and external systems and networks, including the internet. This increases the number of avenues of attack.

Information and systems are subject to serious threats that can have adverse impacts on organizational operations and assets, individuals, other organizations, and the nation. These threats can include purposeful attacks, environmental disruptions, and human/machine errors, and may result in harm to the national and economic security interests of the United States.

In recognition of the growing threat, we have designated information security as a government-wide high-risk area since 1997. In 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure. We further expanded the information

[17]The SOCRATES web-based form is accessible at https://socrates.ocwr.gov/.

security high-risk area in 2015 to include protecting the privacy of personally identifiable information.[18]

Cybersecurity incidents continue to impact federal agencies, including those entities in the federal executive and legislative branch. For example, in fiscal year 2017, federal executive branch civilian agencies reported 35,277 incidents to the U.S. Computer Emergency Readiness Team.[19] These incidents included web-based attacks, phishing,[20] and the loss or theft of computing equipment. These incidents and others like them can pose a serious challenge to economic and national security and personal privacy. The following examples highlight the impact of incidents from legislative and executive branch entities:

- In January 2019, the Department of Justice announced that it had indicted two Ukrainian nationals for their roles in a large-scale, international conspiracy to hack into the Securities and Exchange Commission's computer systems and profit by trading on critical information they stole. The indictment alleges that the two hacked into the commission's Electronic Data Gathering, Analysis, and Retrieval system and stole thousands of files, including annual and quarterly earnings reports containing confidential, nonpublic, financial information, which publicly traded companies are required to disclose to the commission.
- In July 2016, the Library announced that it had experienced a significant distributed denial-of-service attack that affected multiple internal and external Library systems and services.[21] Specifically, the attack successfully disrupted services to multiple Library systems and services including email, databases, and public web domains, such as

[18]For our most recent update on this high-risk area, see GAO-19-157SP.

[19]The U.S. Computer Emergency Readiness Team, a branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, is a central federal information security incident center that compiles and analyzes information about incidents that threaten information security. Federal agencies are required to report such incidents to the U.S. Computer Emergency Readiness Team.

[20]Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

[21]A distributed denial-of-service attack is an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. It is a variant of the denial of service attack that uses numerous hosts to perform the attack.

Congress.gov. According to the Library, the attack was sophisticated in both the size of the attack and methods that the attack employed.

- In June 2015, the Office of Personnel Management 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. In total, the Office of Personnel Management estimated that 22.1 million individuals had some form of personally identifiable information stolen, with 3.6 million being a victim of both breaches.

Key Cybersecurity Management Activities Relevant to OCWR Have Been Established in Law and Guidance

Recognizing the importance of information security and privacy, Congress enacted the Federal Information Security Modernization Act of 2014 (FISMA),[22] which requires federal agencies in the executive branch to develop, document, and implement an information security program and to evaluate the program for effectiveness. The act retains many of the requirements for federal agencies' information security programs previously set by the Federal Information Security Management Act of 2002.[23]

As legislative branch entities, OCWR and the Library are not subject to FISMA. However, OCWR's Executive Director and the Library's Chief Information Officer have chosen to follow aspects of the law's requirements. For example, an interagency agreement between OCWR and the Library describes plans to protect OCWR's CMS application and

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

[23]The Federal Information Security Management Act of 2002 was enacted as *Title III, E-Government Act of 2002,* Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

claim data using NIST guidance that is intended to satisfy FISMA requirements and relates to managing risks to the information system.[24]

The 2002 act also assigns certain responsibilities to NIST, which is tasked with developing standards and guidelines for systems other than national security systems. These standards and guidelines must include, at a minimum, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information system in each category.

Accordingly, NIST developed a risk management framework[25] of standards and guidelines for agencies to follow in developing information security programs.[26] The framework addresses broad information security and risk management activities to be followed in developing information systems, including categorizing the system's impact level; selecting, implementing, and assessing security controls; authorizing the system to operate (based on progress in remediating control weaknesses and an assessment of residual risk); and monitoring the efficacy of controls on an ongoing basis.

[24]NIST, Guide for Applying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37 Revision 1 (Gaithersburg, Md.: February 2010). In December 2018, NIST published updates to its risk management framework in SP 800-37 Revision 2. According to NIST, SP 800-37 is intended to help organizations manage security and privacy risk and to satisfy the requirements in FISMA, among other laws, regulations, and policies.

[25]NIST, SP 800-37, Rev. 2.

[26]As legislative branch entities, OCWR and the Library are not required to follow NIST standards and guidelines. However, OCWR's Executive Director and the Library's Chief Information Officer have chosen to follow these standards and guidelines.

GAO Has Previously Reported on OCWR Project Management Challenges and Information Security Weaknesses within the Library's IT Environment

In December 2019, we reported that OCWR faced management challenges in implementing its new requirements under the Reform Act, such as establishing a program to permanently retain records of investigations, mediations, hearings, and other proceedings.[27] Specifically, we determined that OCWR did not always use project schedules to manage the implementation of the requirements of the Reform Act. For example, we noted that the office used a project schedule for developing the workplace climate survey, but did not use a project schedule to manage the SOCRATES project. We also determined that OCWR did not address risks associated with its records retention program. For example, we noted that the office had not yet developed policies and procedures to address the risks associated with permanently retaining sensitive records, such as ensuring they remain confidential when stored in multiple locations.

Our report also identified weaknesses in OCWR's IT planning, including that the office did not develop long-term strategies for recruiting and retaining staff with critical skills and competencies needed to achieve current and future agency goals. Accordingly, our report included six recommendations for the office related to incorporating key management practices into project planning and ensuring that it has the necessary skills and capacity to meet its mission. OCWR agreed with our recommendations and described plans to address them.

We have also previously reported on weaknesses with the Library's information security program, as well as specific security controls that support OCWR's systems and services.

- In March 2015, we issued a report that identified weaknesses in the Library's information security program.[28] We made 10 recommendations to the Library aimed at better protecting IT systems and reducing the risk that the information they contain will be compromised. These recommendations included, among other things, developing contingency plans for all systems and conducting comprehensive and effective security testing for all systems within the time frames called for by Library policy. The Library generally agreed

[27]GAO, *Office of Congressional Workplace Rights: Using Key Management Practices Would Help to Fully Implement Statutory Requirements,* GAO-20-222 (Washington, D.C.: Dec. 30, 2019).

[28]GAO, *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses,* GAO-15-315 (Washington, D.C.: Mar. 31, 2015).

with our recommendations and described planned and ongoing actions to address them. As of January 2020, the Library fully implemented nine of the 10 recommendations and has taken steps to implement the remaining recommendation. We have work underway to determine whether the steps taken by the Library fully address the remaining recommendation.

- In a related June 2015 limited official use only report, we made 74 detailed security recommendations aimed at addressing specific weaknesses in the Library's security controls. The Library generally agreed with our security recommendations and described planned and ongoing actions to address them as well. As of January 2020, the Library had fully implemented 72 of 74 detailed security control recommendations from this report and had plans to implement the remaining two recommendations by February 2020.

OCWR Did Not Incorporate Key Cybersecurity Management Activities into Project Planning for Its Claim Management System Upgrade

Effectively managing a project entails, among other things, developing a project schedule, defining and managing requirements, and effectively managing project risks.

- **Project scheduling.** The success of a program depends, in part, on having an integrated and reliable master schedule that defines, among other things, when work activities will occur, how long they will take, and how they relate to each other. A reliable schedule provides a road map for systematic execution of a program and a means by which to gauge progress, identify and address potential problems, and promote accountability. GAO's Scheduling Assessment Guide[29] lists 10 best practices associated with a high-quality and reliable schedule, including capturing and sequencing all activities, as well as establishing the duration of all activities.
- **Requirements management.** Requirements establish what the system is to do, how well it is to do it, and how it is to interact with other systems. The Software Engineering Institute's Capability Maturity Model Integration® for Acquisition (CMMI-ACQ)[30] and Capability Maturity Model Integration® for Development (CMMI-

[29]GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules,* GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

[30]Carnegie Mellon University's Software Engineering Institute, *Capability Maturity Model Integration® for Acquisition*, Version 1.3 (CMMI-ACQ V 1.3) (Pittsburgh, Pa.: November 2010).

DEV)[31] note that requirements management processes are important for enabling programs to ensure that their set of approved requirements is managed to support planning and execution needs. This should include steps to obtain stakeholder's review and commitment to the requirements and to manage changes to requirements as customer needs evolve.

- **Project risk management.** The discipline of risk management is important to help ensure that projects are delivered on time, within budget, and with the promised functionality. According to leading practices for acquisition,[32] the purpose of risk management is to identify potential issues that could endanger achievement of critical objectives before they occur. A continuous risk management approach effectively anticipates and mitigates risks that can have a critical impact on a project. Organizations that plan to acquire IT products and services for a project should also identify and assess risks associated with the acquisition process.

Incorporating cybersecurity management activities (such as the selection and implementation of security controls) into each of these project planning areas can help to reduce cybersecurity risks and better protect critical assets. For example, according to NIST's risk management framework, integrating system security requirements into a project's planning activities, such as scheduling, can help to ensure that resources are available when needed and that project milestones are met.[33] In addition, the framework notes that defining the system security requirements early and integrating them with other system requirements can result in a system having fewer deficiencies, and therefore, fewer security vulnerabilities that can be exploited in the future. The framework also describes the importance of identifying security risks early in a system project and addressing such risks on an ongoing basis.

However, OCWR did not effectively manage the SOCRATES project because it did not establish a schedule, develop and manage requirements, and manage risks. Consequently, the office did not

[31]Carnegie Mellon University's Software Engineering Institute, *Capability Maturity Model Integration® for Development*, *Version 1.3* (CMMI-DEV V1.3) (Pittsburgh, Pa.: November. 2010).

[32]CMMI-ACQ V1.3.

[33]NIST, SP 800-37, Rev. 2.

incorporate key cybersecurity management activities into each of these project planning areas. Specifically:

- **OCWR did not manage the SOCRATES project using an established, approved project schedule that identified when cybersecurity activities would be completed.** As discussed earlier, we previously reported that OCWR did not establish a project schedule to manage the SOCRATES project.[34] Although the office drafted a project schedule in January 2019, this schedule was not finalized and used during the project. According to OCWR's Director of the IT Governance, Risk Management, and InfoSec Compliance Program, the schedule was not used due to, among other things, challenges encountered in managing the interdependencies of SOCRATES development with the implementation of other Reform Act requirements (e.g., modifying the administrative dispute resolution process).

  Consequently, OCWR did not use a project schedule to manage key SOCRATES cybersecurity activities, including those to be completed by OCWR, the Library, and the contractor. To its credit, the Library provided an early project schedule with certain cybersecurity activities they performed related to CMS. For example, the Library's project schedule documented initial activities the Library was to perform that related to procurement of equipment, installation of software, security testing, and vulnerability remediation in order to move CMS from OCWR to the Library. However, OCWR did not use a project schedule for the upgrade of CMS to SOCRATES that included the time frames for key cybersecurity management activities, such as selecting and documenting security controls, implementing controls, and assessing controls.

  The lack of a project schedule likely hindered OCWR's ability to respond to changes during the project and execute key cybersecurity management activities in a timely manner. For example, in May 2019, OCWR made a decision to use a locally hosted platform at the Library for its secure information sharing platform instead of a cloud-based solution.[35] Without a project schedule, OCWR was unable to assess

[34]GAO-20-222.

[35]As defined by NIST, cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released.

the impact of this late change on the time available for completing remaining cybersecurity management activities.

- **OCWR did not establish a requirements management process or develop a set of detailed system requirements, including cybersecurity requirements.** OCWR did not establish a requirements management process that included steps to obtain stakeholders' review and commitment to the requirements and to manage changes to the requirements. Instead, the office established a set of business flow diagrams, which identified how claim information would move within OCWR and SOCRATES. Further, OCWR did not establish a set of detailed system requirements, including the cybersecurity requirements (e.g., what cybersecurity controls were to be implemented).
- **OCWR did not document and manage risks to the SOCRATES project, including those related to cybersecurity.** OCWR did not document and manage risks for the SOCRATES project. Specifically, the office did not document and manage risks related to cybersecurity and did not mitigate those risks that could have had a critical impact on the project. For example, OCWR was not able to ensure that the Library tested all moderate-level security controls[36] for the SOCRATES web-based form and secure information sharing platform before the system was deployed. However, this was not documented or managed by OCWR as a risk.

  In addition, as discussed later in this report, there were also risks associated with OCWR's reliance on the Library and its external contractor that were implementing cybersecurity responsibilities on its behalf. For example, we identified shortfalls in the OCWR's oversight of the planning and conducting of system security assessments.

[36]Federal Information Processing Standard Publication 199 (Standards for Security Categorization of Federal Information and Information Systems) establishes security categories for both information and information systems. The security categories (low, moderate, and high) are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Potential impact is considered moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Potential impact is considered high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

However, no risks related to the office's reliance on external parties were documented or managed throughout the project.

According to the Director of the IT Governance, Risk Management, and InfoSec Compliance Program, the office did not complete key project planning activities and documentation, in part, because of the compressed time frame associated with the project and the need to complete it by its mandated June 19, 2019, completion date. In aiming to meet this date, the OCWR official added that they held frequent discussions with the contractor and made changes "on the fly" to ensure that OCWR met the mandate. However, frequent discussions with the contractor does not negate the need to document and manage cybersecurity activities using leading project planning practices, including a project schedule, a requirements management process, and a risk management process.

OCWR's project management weaknesses also occurred, in part, because the office lacked policies and procedures for IT project scheduling, requirements management, and risk management. Such policies and procedures are critical to have in place as OCWR plans future IT projects. For example, as of October 2019, the office was planning to move its other key system, FMA, to the Library in 2020. Until OCWR develops and implements policies and procedures for incorporating cybersecurity management activities into its IT project planning using a project schedule, a requirements management process, and a risk management process, it will continue to have a limited ability to effectively manage and monitor the completion of cybersecurity activities and will face increased cybersecurity risks.

OCWR Did Not Fully Implement Oversight Activities for Selected IT Systems Operated by External Parties on Its Behalf

The responsibility for adequately mitigating risks arising from the use of externally-operated systems remains with the agency itself. NIST Special Publications 800-53[37] and 800-53A[38] guide agencies in selecting security and privacy controls for systems and assessing them to ensure that the selected controls are in place and functioning as expected. Additional NIST special publications on IT security services and risk management (Special Publications 800-35[39] and 800-37[40]) identify several key activities important for assessing the security and privacy controls of information systems operated by external entities. The key activities and the steps included in NIST Special Publications 800-35 and 800-37 are shown in table 2.

Table 2: System Oversight Activities and Key Steps from the National Institute of Standards and Technology (NIST) Special Publications 800-35 and 800-37 (Rev. 2)

Oversight activity	Key steps
Establish security and privacy requirements	**Communicate requirements to external entities.** To ensure that agencies can hold external entities accountable, it is important to establish security requirements with external parties in agreements. The information security and privacy requirements for a system should be communicated in the agreements explicitly or by reference. To ensure that requirements are communicated to external entities, agencies should include information security and privacy language in agreements in sufficient detail to ensure that requirements are communicated effectively.
	Select and document security and privacy controls. Agencies should document in a system security plan the (1) security and privacy requirements that federal employees and contractors should adhere to and (2) a description of the controls in place for meeting those requirements. The security plan also includes and refers to other required security and privacy documentation, such as a privacy impact assessment.
Planning for the security control assessment	**Select an independent assessor.** Agencies should ensure that an assessor is identified and selected to be responsible for conducting the security control assessment. For systems with a moderate- or high-impact level, an independent assessor capable of conducting an impartial assessment of security controls should be used.
	Develop a test plan. Agencies should document within a test plan which controls will be tested and select the appropriate assessment procedures for the system.
Conducting the assessment	**Execute the test plan.** Agencies should ensure that the test plan is appropriately executed and that any controls that do not satisfy the assessment criteria are documented.

[37]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

[38]NIST, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, SP 800-53A, Revision 4 (Gaithersburg, Md.: December 2014).

[39]NIST, SP 800-35.

[40]NIST, SP 800-37, Rev. 2.

Oversight activity	Key steps
Reviewing the assessment results	**Develop plan of action and milestones (POA&M).** If remedial actions are determined to be necessary as part of testing, they should be captured in a POA&M, which records the issue, estimated dates for resolution, and any other information necessary to prioritize the remediation.

Source: GAO analysis of NIST special publications 800-35, Guide to Information Technology Security Services and 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. | GAO-20-199

For the two selected systems—SOCRATES and FMA—OCWR either partially implemented, or did not implement, system oversight activities. Table 3 details the extent to which OCWR implemented system oversight activities and is followed by a discussion of each activity.

Table 3: Extent to Which the Office of Congressional Workplace Rights (OCWR) Implemented System Oversight Activities for the Secure Online Claims Reporting and Tracking E-filing System (SOCRATES) and Facility Management Assistant (FMA)

	Establish security and privacy requirements	Plan assessment of security controls	Conduct assessment	Review assessment
SOCRATES	◐	◐	◐	◐
FMA	◐	○	○	○

Legend: ● = Fully implemented oversight activity. ◐ = Partially implemented some, but not all, of the oversight activity. ○ = Did not implement any aspects of the oversight activity.

Source: GAO analysis of OCWR, Library of Congress, and OCWR external contractor data. | GAO-20-199

- **Establish security and privacy requirements.** OCWR partially implemented this oversight activity for both SOCRATES and FMA.
  - *Communicate requirements to external entities.* OCWR communicated certain security and privacy requirements to its external partners for these two systems. For example, the office's agreements with the Library for SOCRATES stated that the system will be secured in accordance with NIST security guidelines, including Special Publication 800-37,[41] and the Library's security policy guidelines.

    However, OCWR did not always include language in agreements in sufficient detail to ensure that requirements were communicated effectively. For example, the office did not always provide sufficient language to communicate privacy requirements related to the protection of personally identifiable information within its SOCRATES or FMA agreements. Further, OCWR's agreements—related to FMA—expired during our review and contained references to retired Library

[41]NIST, SP 800-37, Rev. 1.

guidelines that are no longer applicable or enforceable with regard to OCWR's external contractor.

- *Select and document security and privacy controls.* OCWR worked with the Library to select and document about 300 security and privacy controls and control enhancements[42] for SOCRATES within a system security plan. Further, the office worked with the Library to support the selection of controls by documenting privacy risks and impacts to SOCRATES within a privacy impact assessment—as called for by NIST to assess the privacy risks associated with collecting and using personal information[43]—that was referred to in the system security plan.

  However, OCWR did not adequately oversee the selection and documentation of security and privacy controls in the system security plan that was used to plan and conduct initial control assessments for SOCRATES. In particular, the office did not always ensure that the system security plan for SOCRATES provided an appropriate description of controls to be implemented to meet the security and privacy requirements.[44] For example, in certain instances, the system security plan described SOCRATES as a low-impact system when describing the security controls used to protect the system. These descriptions differed though from its actual classification as a moderate-impact system, as documented within an interagency agreement between OCWR and the Library. As another example, the system security plan for SOCRATES incorrectly described a security control related to the maintenance of SOCRATES as not applicable to moderate-impact systems. However, NIST's classification of this control describes it as applicable to moderate-impact systems.[45]

[42]According to NIST 800-53, Rev. 4, security control enhancements add functionality, specificity, or strength to base security controls; enhancements are used to provide greater protection than the base security control due to potential adverse organizational impacts or based on assessments of risk.

[43]NIST, SP 800-53, Rev. 4, Appendix J.

[44]Following the March 2019 security control test of the CMS portion of SOCRATES, the system security plan was updated to address certain instances where incorrect control descriptions were documented.

[45]NIST, SP 800-53, Rev. 4

For the FMA system, OCWR relied on its external contractor to document a system security plan that generally described security requirements for the system. However, the plan did not document the privacy requirements or the specific security and privacy controls that were expected to be implemented for FMA as a low-impact system.[46] For example, the plan did not specify an authority to report information to in the event of a security incident. Further, the plan did not include or refer to other necessary security and privacy documentation, such as a privacy impact assessment. As a result, OCWR did not adequately oversee the completion of this key step for its FMA system.

- **Plan assessment of security controls.** OCWR partially implemented this oversight activity for SOCRATES and did not implement it for FMA.
  - *Select an independent assessor.* OCWR relied on the Library to select an assessor for SOCRATES who was independent.[47] For example, for SOCRATES, the Library used an external contractor to initially assess the system and reported taking steps to verify that the assessor was independent from the Library. However, the office did not adequately oversee the completion of this key step for SOCRATES and did not ensure that the assessor used for the system was independent from the office. Specifically, OCWR allowed the Library to select the assessor for SOCRATES and did not take steps to verify the assessor's independence.[48] Further, for FMA, OCWR did not select an assessor to review the system.
  - *Develop a test plan.* Although OCWR relied on the Library to develop a test plan for SOCRATES, the test plan used to conduct

[46]OCWR officials stated that the office categorized FMA as a low-impact system based on a legal rationale related to the CAA. However, the office did not provide evidence of a formal system categorization based on the system's security and privacy risks and requirements.

[47]According to NIST 800-53, Rev. 4, independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness.

[48]We did not evaluate the assessor's independence to ensure it was impartial to OCWR during our review.

initial control testing was not approved by the office and did not specify the procedures that were to be followed to test each control from the SOCRATES system security plan. For example, the SOCRATES test plan specified a high-level procedure for collecting relevant artifacts but did not specify what particular documentation would be collected or reviewed for each control identified in the system security plan. Regarding FMA, OCWR and its external contractor did not develop a test plan.

- **Conduct assessment.** OCWR partially implemented this oversight activity, which includes executing the test plan, for SOCRATES and did not implement it for FMA. Specifically, OCWR worked with the Library to perform initial control testing for SOCRATES and document the results in an online tracking system; however, as previously mentioned, the office did not ensure that a test plan with detailed procedures to test each control was developed and approved prior to the initial testing of SOCRATES. As a result, the office did not adequately oversee the execution of the test plan by the Library to ensure that controls that were assessed as implemented were effectively operating as intended. For FMA, OCWR and its external contractor did not execute a test plan or document the results of any tests for the system.
- **Review assessment.** OCWR partially implemented this oversight activity, which includes developing POA&Ms for remediation of weaknesses, for SOCRATES and did not implement it for FMA. Specifically, OCWR worked with the Library to develop POA&M data for SOCRATES that included many of the recommended NIST elements,[49] such as estimated completion dates and issue identification. For example, following initial control testing in March 2019, OCWR and the Library worked to develop POA&M data for 62 security control weaknesses, including 24 high-risk and 38 moderate-risk weaknesses. As of November 2019, there were seven POA&Ms, including six categorized as high-risk and one as moderate-risk, that OCWR and the Library had not yet addressed.

  However, as previously mentioned, the office did not ensure that a test plan that included detailed procedures to test each control was developed and approved prior to the initial testing of SOCRATES. Therefore, the office could not ensure that controls were tested

[49]According to NIST 800-37, Rev. 2, elements within plans of action and milestones include tasks to be accomplished, milestones established to meet the tasks, and the scheduled completion dates for the milestones and tasks.

appropriately to identify necessary remedial actions in POA&Ms. As a result, OCWR did not adequately oversee the completion of this step and ensure that key POA&Ms were appropriately documented. For FMA, without an executed test plan, OCWR and its external contractor could not complete or update POA&Ms for the system.

According to OCWR officials, including the office's Deputy Executive Director, part of the reason for these shortfalls was that the office did not obtain expertise in security to aid in the completion of these oversight activities until September 2018 when the office hired a new IT Manager. In addition, OCWR officials, including the Deputy Executive Director, could not explain why the contractor did not produce key oversight related artifacts, such as those related to the security testing of controls, as agreed upon in contracts covering FMA during the performance period. However, a key contributing reason that we identified for the shortfalls in OCWR's oversight of external partners was that OCWR had not documented procedures to direct the office in performing such oversight activities effectively.

The lack of documented oversight procedures and shortfalls in OCWR's oversight of its external partners contributed to concerns with the deployment of SOCRATES. For example:

- As previously discussed, OCWR did not ensure that all moderate-level security controls for the SOCRATES web-based form and secure information sharing platform were tested before the system was deployed in June 2019.[50] For example, a control related to testing contingency plans[51] for the SOCRATES web-based form was not assessed until August 2019, approximately 2 months after the system was deployed.
- Although penetration testing[52] of the CMS portion of SOCRATES was completed in May 2019, OCWR did not ensure that penetration

[50]Following the deployment of SOCRATES in June 2019, OCWR worked with the Library to address areas where security controls were not assessed prior to deployment.

[51]According to NIST, a contingency plan is a plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

[52]NIST defines penetration testing as security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers.

testing of the SOCRATES web-based form and secure information sharing platform was conducted before deployment. Penetration testing for the SOCRATES web-based form and secure information sharing platform was subsequently completed in December 2019, approximately 6 months after the system was deployed.

Until OCWR develops and implements effective oversight procedures over its external partners, it may not be able to mitigate risks that could result in the loss of sensitive data or compromise of the office's external systems.

We also assessed selected security controls in place for SOCRATES and FMA including, but not limited to, configuration management, patch management, and personnel security. We intend to issue a separate limited official use only report that discusses the results of this review.

OCWR Has Not Fully Established an Effective Approach for Managing Organization-Wide Cybersecurity Risk

NIST's cybersecurity framework is intended to support federal agencies as they develop, implement, and continuously improve their cybersecurity risk management programs.[53] In this regard, the framework identifies cybersecurity activities for achieving specific outcomes over the lifecycle of an organization's management of cybersecurity risk.[54]

According to NIST, the first stage of the cybersecurity risk management lifecycle—which the framework refers to as "identify"—is focused on foundational activities for effective risk management that provide agencies with the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. Additional NIST guidance, including its risk management framework, provides information on implementing foundational activities and achieving desired outcomes that calls for, among other things, the following:[55]

[53]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (April 16, 2018).

[54]According NIST's cybersecurity framework, there are five stages in the cybersecurity risk management lifecycle: identify, protect, detect, respond, and recover. They are intended to aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

[55]NIST, SP 800-53, Rev. 4; NIST, *Managing Information Security Risk: Organization, Mission, and Information System View,* SP 800-39 (Gaithersburg, Md.: March 2011); NIST, SP 800-37, Rev. 2.

- **A risk executive** in the form of an individual or group that provides agency-wide oversight of risk activities and facilitates collaboration among stakeholders and consistent application of the risk management strategy. This functional role helps to ensure that risk management is institutionalized into the day-to-day operations of organizations as a priority and integral part of carrying out missions.
- **A cybersecurity risk management strategy** that articulates how an agency intends to assess, respond to, and monitor risk associated with the operation and use of the information systems it relies on to carry out the mission. The strategy should, among other things, make explicit an agency's risk tolerance,[56] accepted risk assessment methodologies, a process for consistently evaluating risk across the organization, risk response strategies, approaches for monitoring risk over time, and priorities for investing in risk management.
- **Risk-based policies and procedures** that act as the primary mechanisms through which current security requirements are communicated to help reduce the agency's risk of unauthorized access or disruption of services. If properly implemented, these policies and procedures may be able to effectively reduce the risk that could come from cybersecurity threats such as unauthorized access or disruption of services. For example, establishing policies and procedures that incorporate NIST's risk management framework can help to ensure that a consistent approach is used to conduct a complete security assessment before a system is deployed and that a designated agency official certifies the system for operation based on progress in remediating control weaknesses and an assessment of residual risk.[57]

To its credit, OCWR's strategic plan for fiscal years 2019 through 2023 includes a goal of developing, among other things, cybersecurity risk policies and procedures. The strategic plan also describes the office's

[56]Risk tolerance is the level of risk or degree of uncertainty that is acceptable to organizations. It affects the nature and extent of risk management oversight, the extent and rigor of risk assessments performed, and the context of organization strategies for responding to risk.

[57]NIST, SP 800-37, Rev. 2. As previously mentioned, NIST's risk management framework addresses broad information-security and risk-management activities to be followed in developing information systems, including categorizing the system's impact level; selecting, implementing, and assessing security controls; authorizing the system to operate; and monitoring the efficacy of controls on an ongoing basis.

plans to ensure compliance with applicable IT and cybersecurity standards.

Nevertheless, OCWR has not yet fully established an effective approach to organization-wide cybersecurity risk management that includes foundational elements. Specifically, although the office's Director of the IT Governance, Risk Management, and InfoSec Compliance Program stated that he was serving as the risk executive, this role and its related responsibilities are not documented in OCWR's policies. In addition, OCWR has not developed an organization-wide cybersecurity risk management strategy or determined a time frame for when the policies and procedures discussed in its strategic plan will be implemented.

According to the Director of the IT Governance, Risk Management, and InfoSec Compliance Program, the reason for these shortfalls in risk management was that the office's top priority was completing work on the SOCRATES system, and then it planned to work on its cybersecurity policies and procedures. Additionally, the official stated that OCWR considers development of documentation to be a continual process, and that the office would like to develop and build procedures to lay a foundation for effective risk management.

However, until OCWR establishes the role and responsibilities of the risk executive function in policy, the office will lack an understanding of who is ultimately responsible for overseeing the cybersecurity risk activities of the organization and what those responsibilities include. Further, until OCWR establishes and implements a strategy for managing its cybersecurity risks using NIST's framework, its ability to make operational decisions that adequately address security risks and prioritize IT security investments will be hindered. Finally, until OCWR establishes a time frame for developing and implementing risk-based policies and procedures, it will lack assurance that consistent steps are being taken to categorize systems; select, implement, and assess system security controls; and make risk-based decisions on authorizing systems to operate.

Conclusions

Although OCWR completed the upgrade of its legacy claims management system through the SOCRATES project, the office did not incorporate cybersecurity activities into the project during planning. As a result, OCWR was left without a complete understanding of potential schedule issues, the system's planned security requirements, and cybersecurity-related risks to the success of the project. These shortcomings existed, at

least in part, because of a lack of OCWR policies and procedures that required cybersecurity management activities be incorporated into project scheduling, requirements management, and risk management. Until OCWR develops and implements such policies and procedures, future IT projects—such as the office's planned transition of its FMA system to the Library—may face unnecessary cybersecurity risks and may not be carried out in an efficient and effective manner.

OCWR made initial efforts to assess the implementation of security and privacy controls for the two selected externally-operated systems, but did not fully implement critical oversight activities. A contributing reason for these shortfalls is that OCWR had not documented procedures for the office to follow in order to perform such oversight of its external entities effectively. This ultimately contributed to OCWR not being able to first test important system security controls for ensuring the confidentiality, integrity, and availability of the system before it was deployed. Until OCWR establishes and implements specific procedures for overseeing external entities, it will have reduced assurance that external entities are adequately securing and protecting the office's information. In addition, the office will face increased risks that system weaknesses may go undetected and unresolved, which could result in the loss of sensitive data or compromise of its systems.

Given the increasing number and sophistication of cyber threats facing federal agencies, it is critical that organizations such as OCWR are well positioned to make consistent, informed risk-based decisions in protecting their systems and information against these threats. To its credit, OCWR has recognized the need for an improved organization-wide approach to its cybersecurity policies and IT governance in its most recent strategic plan. However, important elements of an effective organization-wide cybersecurity approach have not been fully implemented, including establishing the roles and responsibilities for the risk executive function in policy, a cybersecurity risk management strategy, and policies and procedures for managing cybersecurity risks. Until OCWR fully addresses these organization-wide cybersecurity risk management practices, its ability to ensure effective oversight and management of IT will remain limited. Moreover, OCWR may be limited in its ability to strengthen its risk posture, including ensuring effective cybersecurity across its relationships with external entities that are critical to its ability to provide IT services and systems needed to meet its mission.

Recommendations

We are making five recommendations to the Office of Congressional Workplace Rights:

The Executive Director should ensure the development and implementation of policies and procedures for incorporating key cybersecurity activities into IT project planning, including scheduling, requirements management, and risk management. (Recommendation 1)

The Executive Director should ensure the development and implementation of oversight procedures for each externally-operated system that include

- establishing security and privacy requirements,
- planning the assessment of security controls,
- conducting the assessment, and,
- reviewing the assessment. (Recommendation 2)

The Executive Director should ensure the establishment of roles and responsibilities for a risk executive function. (Recommendation 3)

The Executive Director should ensure the development and implementation of a cybersecurity risk management strategy. (Recommendation 4)

The Executive Director should ensure commitment to a time frame for developing and implementing policies and procedures for managing cybersecurity risk. (Recommendation 5)

Agency Comments, Third-Party Views, and Our Evaluation

We provided a draft of this report to OCWR, the Library, and the third-party contractor for review and comment. In response, we received written comments from OCWR, which are reproduced in appendix II. In its comments, the office did not state whether it agreed or disagreed with our recommendations, but described initial actions taken and planned to address them. Specifically, OCWR noted that it has initiated several actions, such as revising the office's IT systems project planning to ensure the development and implementation of policies and procedures incorporating key cybersecurity activities. Further, OCWR stated that it intends to implement additional changes, such as developing and implementing oversight procedures for each externally-operated system. Going forward, OCWR stated that it intends to update us on its progress in implementing the recommendations.

We also received technical comments from the Library's Deputy Chief Information Officer via email, which we incorporated as appropriate. In addition, the third-party contractor indicated via email that it had no concerns about, and worked with OCWR in responding to, the draft report.

We are sending copies of this report to the appropriate congressional committees, the Executive Director of the Office of Congressional Workplace Rights, the Librarian of Congress, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9342 or marinosn@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.

Nick Marinos
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to examine the extent to which the Office of Congressional Workplace Rights (OCWR) (1) incorporated key cybersecurity management activities into the 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 organization-wide approach for managing cybersecurity risk.

To assess OCWR's incorporation of key cybersecurity management activities into the project planning for its claim management system upgrade (known as the Secure Online Claims Reporting and Tracking E-filing System, or SOCRATES), we reviewed available OCWR project planning documentation related to establishing a project schedule, requirements management process, and risk management process. This documentation included, for example, a draft SOCRATES project schedule, contract information, and business flow diagrams. We then compared OCWR's documentation to leading practices for project planning, including those identified by the Software Engineering Institute.[1] Three key areas needed to effectively managing projects are developing a project schedule;[2] managing project requirements;[3] and managing project risks.[4]

We also analyzed OCWR's available project planning documentation to determine the extent that it incorporated key cybersecurity management activities, as identified by the National Institute of Standards and Technology (NIST) risk management framework.[5] These key activities are: obtaining a system categorization, selecting and implementing

[1]The Software Engineering Institute is a federally funded research and development center whose mission is to advance software engineering and related disciplines to ensure the development and operation of systems with predictable and improved cost, schedule, and quality.

[2]GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules,* GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

[3]Carnegie Mellon University's Software Engineering Institute, *Capability Maturity Model Integration® for Acquisition*, *Version 1.3* (CMMI-ACQ® V1.3) (Pittsburgh, Pa.: November 2010) and *Capability Maturity Model Integration® for Development*, *Version 1.3* (CMMI-DEV® V1.3) (Pittsburgh, Pa.: November 2010).

[4]CMMI-ACQ V 1.3.

[5]NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* Special Publication (SP) 800-37, Revision (Rev.) 2 (Gaithersburg, Md.: December 2018).

security controls, assessing security controls, obtaining an authority to operate, and monitoring of security controls. Further, we conducted interviews with OCWR officials, including the General Counsel and the Director of the Information Technology (IT) Governance, Risk Management, and InfoSec Compliance Program, to assess the extent to which the office incorporated key cybersecurity management activities into its SOCRATES project planning.

To assess the extent to which OCWR performed oversight of security controls and mitigated risks for selected externally-operated systems, we chose two systems—SOCRATES and the Facility Management Assistant (FMA). We chose these two systems because they process and maintain OCWR's most sensitive information,[6] including claims related to alleged violations of employee rights and protections and reported occupational safety and health violations.[7] We then collected and reviewed cybersecurity policies, procedures, and documentation (e.g., system security plans) from the office and its external partners that related to protecting the security and privacy of information and systems.

To assess the reliability of the SOCRATES system security plan and its security control testing data obtained from the Library's online repository, we reviewed related documentation (e.g., security assessment results briefings), reviewed the data for obvious omissions (i.e., fields left blank), and performed electronic testing to identify outliers. We also interviewed Library officials to discuss the reliability of the data. Based on our assessment, we determined that the data were sufficiently reliable for the purpose of our reporting objectives.

We then examined whether OCWR and its external partners implemented—for each selected system—four oversight activities important for assessing the security and privacy controls of information systems operated by external entities, as specified in federal

[6]OCWR also uses a third externally-operated system for, among other things, accessing information related to the Americans with Disabilities Act of 1990 (e.g., accessibility standards). According to OCWR's General Counsel, this system contains information reproduced in publicly available reports.

[7]Reported occupational health and safety violations may contain sensitive information related to vulnerabilities in legislative branch facilities (e.g., fire safety) that could be exploited to exacerbate the harm caused by a physical attack.

requirements and guidance, including NIST Special Publications 800-35,[8] and 800-37.[9] The four oversight activities we examined were: (1) establishing security and privacy requirements, (2) planning the assessment of security controls, (3) conducting the assessment, and (4) reviewing the assessment. We chose these activities because of their importance to providing effective oversight of systems operated by external entities.

Further, we assessed whether OCWR implemented policies and procedures set forth by the office, including contractor oversight activities performed by the responsible official. We also conducted interviews with officials from OCWR, including the General Counsel, Deputy Executive Director, and Director of the IT Governance, Risk Management, and InfoSec Compliance Program. In addition, we also interviewed key personnel from OCWR's external partners, such as the Library's Deputy Chief Information Officer and the President of the external contractor, to assess the extent of OCWR's oversight activities for SOCRATES and FMA.

We assessed selected security controls in place for SOCRATES and FMA including, but not limited to, configuration management, patch management, and personnel security. We intend to issue a separate limited official use only report that discusses the results of this review.

To assess OCWR's efforts to establish an effective organization-wide approach for cybersecurity risk management activities, we used NIST's cybersecurity framework,[10] which identifies foundational components of effective cybersecurity risk management. We also used additional guidance provided by NIST for implementing the foundational components and achieving desired outcomes.[11] These components included the establishment of a risk executive function, cybersecurity risk management strategy, and risk-based security policies and procedures.

[8]NIST, *Guide to Information Technology Services*, SP 800-35 (Gaithersburg, Md.: October 2003).

[9]NIST, SP 800-37, Rev. 2.

[10]NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018).

[11]NIST, SP 800-53, Rev. 4; NIST, *Managing Information Security Risk: Organization, Mission, and Information System View,* SP 800-39 (Gaithersburg, Md.: March 2011); NIST, SP 800-37, Rev. 2.

We then evaluated OCWR's organization-wide cybersecurity risk management approach by, among other things, analyzing available policies and plans, management reports, and strategic planning documentation against the foundational cybersecurity risk management components identified in NIST guidance. Further, we conducted semistructured interviews with relevant OCWR officials with responsibilities for managing their efforts to establish an approach for managing cybersecurity risk, including the General Counsel and the Director of the IT Governance, Risk Management, and InfoSec Compliance Program.

We conducted this performance audit from January 2019 to February 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Office of Congressional Workplace Rights

Office of Congressional Workplace Rights

January 21, 2020

Mr. Nick Marinos
Director
Information Technology & Cybersecurity
United States General Accountability Office
441 G Street NW
Washington, D.C. 20548

Re: Draft Report on OCWR Cybersecurity Management

Dear Mr. Marinos:

Thank you for the opportunity to comment on the draft of the GAO Report reviewing OCWR's cybersecurity management as required by the CAA Reform Act of 2018. We realize that our very small office has been understaffed and underfunded in the area of cybersecurity for many years and greatly appreciate the opportunity to work with your office and our oversight committees to acquire the necessary cybersecurity expertise to provide more robust management of the protections being provided to our IT systems. We have reviewed your recommendations and are in the process of taking the following steps to address each of them:

1. With respect to Recommendation 1, as indicated in our response to a similar recommendation made in your report reviewing OCWR management practices, we are in the process of revising our IT systems project planning to ensure the development and implementation of policies and procedure incorporating key cybersecurity activities. We have created and will be filling the position of IT Security Project Manager to acquire the necessary cybersecurity expertise needed to implement this recommendation and to ensure that sufficient time and resources can be dedicated to the development and implementation of these policies and procedures.

2. With respect to Recommendation 2, we will be working with the IT Security Project Manager and the IT Risk Executive to develop and implement oversight procedures for each externally-operated system.

3. With respect to Recommendation 3, we have expanded the OCWR IT Director's role to formally include the functions of an IT Risk Executive and are in the process of establishing the roles and responsibilities.

Room LA 200, Adams Building · 110 Second Street, SE · Washington, DC 20540-1999 · t/202.724.9250 · f/202.426.1913

www.ocwr.gov

4. With respect to Recommendation 4, we will be working with the IT Security Project Manager and the IT Risk Executive to ensure the development and implementation of a cybersecurity risk management strategy.

5. With respect to Recommendation 5, once the position of IT Security Project Manager is filled and the IT Risk Executive functions are formalized, we will develop and commit to a time frame for developing and implementing policies and procedures for managing cybersecurity risk.

We appreciated the opportunity to work with your very knowledgeable team on this project. We will provide you with updates as we make further progress on implementing the recommendations.

Very truly yours,

Susan Tsui Grundmann
Executive Director

Room LA 200, Adams Building · 110 Second Street, SE · Washington, DC 20540-1999 · t/202.724.9250 · f/202.426.1913

www.ocwr.gov

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contact

Nick Marinos, (202) 512-9342 or marinosn@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jon Ticehurst (Assistant Director), Lisa Hardman (Analyst in Charge), Edward Alexander, Jr., Angela Bell, Christina Bixby, David Blanding, Hannah Brookhart, Kisa Bushyeager, Christopher Businsky, West Coile, Linda Erickson, Rebecca Eyler, Kaelin Kuhn, Sukhjoot Singh, Eugene Stevens, and Adam Vodraska made key contributions to this report. Giny Cheong, Edda Emmanuelli-Perez, Elizabeth Fan, Steven Lozano, Rebecca Woiwode, and Edith Yuh also provided valuable assistance.

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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

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, https://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, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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