Office of Inspector General
U.S. Government Accountability Office

INFORMATION ON GOVERNMENT ACCOUNTABILITY OFFICE COVERED COMPUTER SYSTEMS PURSUANT TO THE CYBERSECURITY ACT OF 2015

Serving the Congress and the Nation

August 2016

OIG-16-4

O I G
Office of Inspector General

United States Government Accountability Office
441 G Street NW, Room 1808
Washington, DC 20548

August 3, 2016

The Honorable Ron Johnson
Chairman
The Honorable Thomas Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
U.S. Senate

The Honorable Jason Chaffetz
Chairman
The Honorable Elijah Cummings
Ranking Member
Committee on Oversight and Government Reform
U.S. House of Representatives

Information on Government Accountability Office Covered Computer Systems Pursuant to the Cybersecurity Act of 2015

The Cybersecurity Act of 2015[1] requires Inspectors General to report on federal computer systems that are national security systems or that provide access to personally identifiable information.[2] This report satisfies the requirement for the Government Accountability Office (GAO). Because GAO has no national security systems, our report is specific to its computer systems that provide access to personally identifiable information (PII).

Our objective was to collect specific information on GAO's information security policies and practices governing systems that provide access to PII and to assess whether logical access policies and practices over these systems are appropriate and were being followed. We did not independently validate the information that GAO provided for this report, except to determine that appropriate logical access standards and guidance were being followed, as required.

To assess whether GAO's information security policies and practices are appropriate and were being followed, we analyzed GAO's access policies and practices and compared them to applicable guidance[3] from the Office of Management and Budget (OMB) and National

[1]Consolidated Appropriations Act of 2016, Pub. L. 114-113, Div. N (Dec. 18, 2015) (Cybersecurity Act of 2015).

[2]The Act requires this report to be submitted to the appropriate committees of jurisdiction in the Senate and the House of Representatives no later than 240 days after the enactment of the Act.

[3]OMB, *Memorandum for the Heads of Executive Departments and Agencies: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*, M-11-11 (Washington, D.C.: Feb. 3, 2011)

Institute of Standards and Technology (NIST) standards[4] related to identity and access management. We also reviewed log-ins and performed other steps to verify that systems identified in GAO's systems inventory at the time of our audit were in compliance with GAO's logical access policies and practices, as appropriate. In addition, we reviewed prior reports on GAO's information security issued by our office and GAO's financial statement auditors and considered the status of any open recommendations from those reports that were relevant to logical access. We also interviewed GAO personnel responsible for operating and overseeing covered systems. We obtained oral comments from GAO regarding our assessment of its compliance with logical access standards, which we incorporated, as appropriate.

This report covers the results of our assessment of logical access controls and GAO's responses to our information requests.

We conducted this performance audit from April 2016 to August 2016 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.

A. A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

GAO Response: The GAO Infrastructure, GAO's primary general support system, is the backbone upon which GAO's systems and applications maintaining personally identifiable information (PII) rely. Specifically, these systems rely on the safeguards in place for logical access and multi-factor authentication. Furthermore, they rely on the various inventory, licensing, monitoring, and defense-in-depth security services provided by the GAO Infrastructure.

GAO systems that provide access to PII can be described as those systems that support GAO's human capital, financial, and engagement management efforts. Examples of systems supporting such efforts would be the performance management, time and attendance, and bid protest management, respectively.

From a logical access perspective, GAO has established a standard for multi-factor authentication, using an RSA token.

Users are first required to authenticate to GAO-issued workstations using two-factor authentication, then they will have access to the GAO infrastructure. Systems require the use of the RSA token for users to access the systems. Once the end users have authenticated, users are provided access to information based upon their roles to systems that provide access to PII.

[4]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013) and NIST, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, SP 800-53A, Revision 4 (Gaithersburg, Md.: Dec. 2014).

OIG Comment: GAO's logical access policies and practices established at the time of our review are appropriate and were being followed. For this audit, we reviewed the log-in screens and analyzed network access controls and file permissions for individual systems GAO identified as collecting, storing, or maintaining personally identifiable information. We found that all the systems reviewed used multi-factor authentication, as well as additional controls, to control access.

We also evaluated GAO's *Network Account Management Policy and Procedures* using NIST standards and guidance.[5] Specifically, we identified key areas related to access controls that should be documented within an agency's policy and procedures, including: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. We then analyzed GAO's policy and procedures and concluded that GAO had adequately addressed these key areas in its policies and procedures.

Finally, we reviewed recent information security assessment reports, including our own and those of other auditors, and obtained the status of recommendations or issues identified regarding access controls. For example, we reviewed GAO's information security program in voluntary compliance with Federal Information Security Management Act (FISMA) requirements every year except 2013. As stated in our March 2016 report,[6] GAO uses multi-factor authentication for controlling workstation and network access, as well as access to several applications. This multi-factor authentication consists of a password; a random sequence of log-in numbers generated by a security access token provided to each user; and a personal identification number that is uniquely tied to the token. GAO also has a policy to encrypt sensitive data in electronic mail attachments.

GAO's financial statement audits identified two contractor network accounts in fiscal year 2011 and four contractor network accounts in 2012 that were not deleted in accordance with GAO separation procedures. In fiscal year 2014, as a follow-up to its prior findings, GAO's financial statement auditor recommended that GAO management finalize and implement policy (currently draft GAO Order 2300.3, "Exit Clearance Procedures for Personnel Separating from GAO") and supporting procedures for incoming and outgoing federal employees and contractors related to logical and physical access, property accountability, training, and other administrative matters.[7] As of August 1, 2016, GAO had not yet finalized and implemented its policy to address the recommendation.

[5]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013) and NIST, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, SP 800-53A, Revision 4 (Gaithersburg, Md.: Dec. 2014).

[6]OIG, *Information Security: Review of GAO's Program and Practices for Fiscal Years 2014 and 2015*, OIG-16-2 (Washington, D.C.: Mar. 28, 2016).

[7]CliftonLarsonAllen LLP, *Management Letter to the Comptroller General of the United States* (Calverton, Md.: Nov. 14, 2014).

B. A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

GAO Response: All access to the GAO network and endpoint workstations is governed by GAO's multi-factor authentication practices.

GAO is in the process of implementing a Privileged Account Manager to provide more effective security around the use of these account types which will require two-factor authentication to access their privileged account password.

To mitigate the transition to a Privileged Account Manager, GAO has ensured that such privileged users have established a strong password that is required to be protected by having their password refreshed routinely.

OIG Comment: We did not independently analyze or validate the data provided for this section of the report.

C. If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

GAO Response: As previously noted, however, all access to the GAO network and endpoint workstations is governed by GAO's multi-factor authentication practices.

GAO is in the process of implementing a Privileged Account Manager to provide more effective security around the use of these account types which will require two-factor authentication to access their privileged account password.

To mitigate the transition to a Privileged Account Manager, GAO has ensured that such privileged users have established a strong password that is required to be protected by having their password refreshed routinely.

OIG Comment: We did not independently analyze or validate the data provided for this section of the report.

D. A description of the following information security management practices used by the covered agency regarding covered systems:

(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

(I) data loss prevention capabilities;

(II) forensics and visibility capabilities; or

(III) digital rights management capabilities.

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

GAO Response: Commercial software products present within the GAO Infrastructure are managed and tracked by budget and acquisitions management staff to ensure that software updates and licenses for the products are tracked and maintained. Furthermore, the addition of technology within the environment is governed by the GAO's Change Advisory Board or by the Chief Information Officer as part of the budget approval and project management processes.

GAO has implemented defense-in-depth IT security controls at the GAO Infrastructure's perimeter, the network, and on the users' desktops to detect malicious behavior and activities.

GAO has implemented several security tools as no "one" security tool provides complete coverage to prevent and detect data loss. Specifically, these tools have the capability to block detected malicious activity, detect malicious activity on the network or on endpoint devices, including servers, providing an early warning and quarantine capability. Once detected, these tools provide a plethora of capabilities to analyze the malicious content and determine effective remediation efforts.

GAO has started the implementation of a data loss technology to help determine the breadth of information, specifically, PII that resides across the agency within and outside of specific information systems.

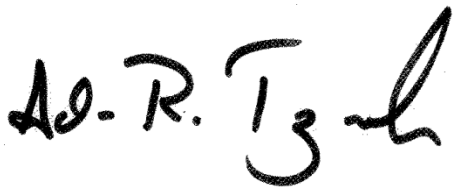
OIG Comment: We did not independently analyze or validate the data provided for this section of the report.

E. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

GAO Response: GAO's standard staff and contractor onboarding process for network access reinforces the information security management practices outlined in subparagraph D. Furthermore, each contractor has agreed to follow GAO's information security management practices and IT governance practices for Change Management.

OIG Comment: We did not independently analyze or validate the data provided for this section of the report.

Thank you for the opportunity to contribute to your efforts to improve federal network and information system security. If you need additional information or would like to discuss our responses, please contact me at (202) 512-5748 or trzeciaka@gao.gov.



Adam R. Trzeciak
Inspector General

Reporting Fraud, Waste, and Abuse in GAO's Internal Operations

To report fraud and other serious problems, abuses, and deficiencies relating to GAO programs and operations, do one of the following. (You may do so anonymously.)

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Online at: https://OIG.alertline.com.

Obtaining Copies of OIG Reports and Testimony

To obtain copies of OIG reports and testimony, go to GAO's website: www.gao.gov/about/workforce/ig.html or call (202) 512-5748.

OIG

Office of Inspector General
U.S. Government Accountability Office