Office of Inspector General

AUG 12 2016

MEMORANDUM FOR THE ADMINISTRATOR

FROM: Ann Calvaresi Barr
Inspector General

SUBJECT: Cybersecurity Act of 2015 Report

The Cybersecurity Act of 2015, Public Law 114-113, Section 406, requires the inspector general of every agency that operates a Federal national security system or a Federal system that provides access to personally identifiable information (PII) to report the following information on the computer systems' security controls and practices:

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

- A description and list of the logical access controls and multifactor authentication the agency uses to govern privileged users' access to covered systems.

- If the agency does not use logical access controls or multifactor authentication to access a covered system, the reasons why it does not use them.

- A description of the agency's information security management practices for the covered systems.

- A description of the agency's policies and procedures to ensure that entities providing services to the agency, including contractors, implement the information security management practices.

Our report on USAID's information systems is enclosed. While USAID does not operate a national security system as described in Section 406, it does operate systems with access to PII. The independent certified public accounting firm CliftonLarsonAllen LLP prepared this report

drawing on fieldwork it performed during its audit of USAID's fiscal year 2016 Federal Information Security Modernization Act (FISMA) compliance. Any deficiencies related to USAID's logical access policies, practices, or controls will be included in our audit report on FISMA compliance later this year.

We have redacted sensitive but unclassified information pertaining to USAID's information security practices from the attached responses pursuant to Freedom of Information Act exemption 7(E), 5 U.S.C. § 552(b)(7)(E) and 12 FAM 541 (b)(5) (i.e., information disclosing vulnerabilities in USAID systems).

If you have any questions about our work, please contact me directly, or members of your staff may contact our Assistant Inspector General for Audit, Thomas Yatsco at 202-712-1150.

Enclosure

CliftonLarsonAllen LLP
www.claconnect.com

July 11, 2016

Mr. Mark Norman
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20005-2221

Dear Mr. Norman:

The USAID Office of Inspector General tasked CliftonLarsonAllen LLP to assist in meeting its requirements to respond to Section 406(b)(2) of the Cybersecurity Act of 2015 for the U.S. Agency for International Development (USAID). Enclosed are our responses.

In addressing the requirements, we leveraged the audit procedures performed during our current audit of USAID's compliance with the Federal Information Security Modernization Act of 2014 (FISMA). To address requirements that were not reviewed as part of the FISMA audit, we assessed additional controls identified in National Institute of Standards and Technology's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

The attached responses do not provide any conclusions or recommendations. Our overall conclusions and recommendations will be noted in the USAID FISMA audit report for fiscal year 2016.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Very truly yours,

CLIFTONLARSONALLEN LLP

Response to Section 406(b)(2) of the Cybersecurity Act of 2015

The following presents responses to Section 406(b)(2) of the Cybersecurity Act of 2015 for the U.S. Agency for International Development (USAID) for the following selected covered systems: Agency for International Development Network (AIDNet), Phoenix Financial System, Global Acquisition and Assistance System (GLAAS), WebTA, and Enterprise Loan Management System (ELMS).

CyberSecurity Act of 2015 - Inspector General Reports On Covered Systems
Excerpt from Section 406(b):

(2) CONTENTS - The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:

(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.

Response:
USAID's logical access policies and procedures are documented in the *Automated Directive System (ADS) Chapter 545, Information Systems Security Policy*, dated March 9, 2016. The access control policies and practices cover procedures for establishing, modifying, and reviewing system user accounts. In addition, the policies include procedures related to segregation of duties, remote access, least privilege, and access enforcement.

~~(SBU)~~ USAID requires all users to have an approved user access request form, signed rules of behavior, and completed security awareness training prior to being granted access to USAID's network (AIDNet). Based on testing completed for a sample of AIDNet users, we noted the following:

[redacted]

~~(SBU)~~ User accounts are reviewed for inactivity and disabled after 90 days of inactivity. In addition, user accounts are reviewed on an annual basis. Terminated/separated user accounts are disabled upon personnel termination. [redacted]

USAID configures all accounts with the concept of segregation of duties and least privilege. To gain privileged access to the network, a user must complete the privileged access request form and have it reviewed and approved by the Authorizing Official. USAID also requires administrators to use different credentials to perform their administrative tasks.

All USAID users are granted the ability to connect to the AIDNet Network remotely. Users are required to access the network remotely through USAID's

Server Based Computing (SBC) implementation of a Citrix website using their "user name", a pin number, and password along with their RSA token for multi-factor authentication. USAID has configured workstations to lock out user accounts after 3 invalid login attempts for a duration of 20 minutes to reduce the likelihood of unauthorized access to the network.

To gain access to the Phoenix Financial System, users must complete the specific Phoenix User/Role Request Form and sign the Phoenix Access Request Acknowledgement.

USAID has documented a segregation of duties matrix for the Phoenix system which is checked when new user accounts, including administrator accounts, are created to ensure the permissions assigned to the account do not pose any segregation of duties conflicts. Phoenix user and administrator accounts are also configured with the principle of least privilege and granted the most restrictive set of permissions necessary for the user to complete their job responsibilities.

Phoenix accounts are monitored and disabled with an automated script after 90 days of inactivity. In addition, Phoenix accounts are reviewed and recertified on a triennial basis. The recertification requires Washington Bureaus and Missions to review and resubmit access request forms for all the users in year one and two. Year three is an off year. Terminated/separated user accounts are disabled upon personnel termination.

To gain access to the Global Acquisition and Assistance System (GLAAS), users must complete the specific GLAAS User/Role Access Form and sign the GLAAS Access Agreement Form.

USAID has documented a segregation of duties matrix for the GLAAS system which is checked when new user accounts, including administrator accounts, are created to ensure the permissions assigned to the account do not pose any segregation of duties conflicts. GLAAS user and administrator accounts are also configured with the principle of least privilege and granted the most restrictive set of permissions necessary for the user to complete their job responsibilities.

GLAAS accounts are monitored and disabled within an automated script after 90 days of inactivity. In addition, user accounts are reviewed on an annual basis. Terminated/separated user accounts are disabled upon personnel termination.

~~(SBU)~~ To gain access to WebTA, users are required to have access to AIDNet because it uses single sign-on technology. Timekeepers are responsible for adding and removing employees in WebTA for their respective USAID Mission or Washington bureau. WebTA requires administrator accounts to be reviewed and approved by the Payroll Division Chief within the Office of the Chief Financial Officer. [redacted] In addition to signing a Rules of Behavior Form when obtaining access to AIDNet, WebTA users are also required to accept the terms and conditions prior to entering the WebTA system. [redacted]

[redacted]

USAID has documented a segregation of duties matrix for the WebTA system which is implemented within the application to ensure the permissions assigned to an account do not pose any segregation of duties conflicts. Depending on the role selected, conflicting roles are grayed-out and not available for selection in the system. WebTA user accounts are also configured with the principle of least privilege and granted the most restrictive set of permissions necessary for the user to complete their job responsibilities. In addition, WebTA application rules do not allow an employee to self-certify their own timesheet. Based on testing completed, users were identified with the "Supervisor" and "Self-Certify" roles within system. However, in accordance with Government Accounting Office 03-352G, *Internal Control Maintaining Effective Control over Employee Time and Attendance Reporting,* dated January 2003, certain positions are exempt from the rule such as presidential appointees with Senate confirmation, Mission Directors, and Directors of Independent Offices (or career employees detailed to these position), who must certify their own bi-weekly time and attendance in WebTA.

~~(SBU)~~ The Enterprise Loan Management System (ELMS) is an external system. USAID contracted with Midland Loan Services, a division of PNC Financial Services Group Inc., to handle the administration of loans and foreign currency transactions within USAID's financial portfolio. USAID is only responsible for tracking when it requests user account access for ELMS and when it requests a user account to be terminated. To request and remove access to ELMS, [redacted]

(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.

Response:
USAID currently has logical access controls in place for privileged users. USAID requires privileged users to have two domain accounts. One is their normal user account for their day-to-day activities. The second is an elevated privilege account which they use to perform actions requiring administrative access. To be granted access to a privileged account the user must fill out an administrative privileges request form which is reviewed and approved by the Authorizing Official.

Multifactor authentication is fully implemented for network and local access to privileged accounts. For personnel within the Continental United States all privileged accounts are required to use Personal Identification Verification cards to obtain access to the information system. For USAID missions, a Personal Identification Verification-Alternative is required for logical access to the network. Personal Identification Verification-Alternative is a Personal Identification

Verification card without a picture and is linked to the individual's USAID AIDNet username. Executive Officers for the USAID mission are the Local Representative Authority and are responsible for issuing Personal Identification Verification-Alternative cards to users.

(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.

Response:
Not applicable. USAID is using logical access controls and multi-factor authentication for privileged and non-privileged users.

(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.

Response:
USAID has documented procedures on conducting software inventory in the *Operation and Maintenance of USAID's Information Technology Infrastructure and Systems Program (O&M IT IS) Asset Management: Software and Hardware Maintenance Renewal and New Purchase* dated May 24th, 2016.

(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.

Response:
For data loss prevention, USAID has capabilities to detect and prevent the unauthorized disclosure of sensitive information. For example, USAID can inspect outbound email and generates alerts based on a set of designated criteria including Personally Identifiable Information (PII) elements. In addition, USAID can monitor and detect malicious activities on the USAID network from internal and external entities.

Regarding forensic and visibility capabilities, USAID can investigate any threat entering or attempting to enter its network. In addition, USAID can monitor and detect malicious activities on the network.

For digital rights management, USAID has the capability to conduct automated inventories of the software on the network.

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

Response:
~~(SBU)~~ USAID has implemented [redacted] which is designed to detect and prevent the unauthorized disclosure of sensitive information. The [redacted] system inspects outbound email and generates alerts based on a set of designated criteria including PII elements, such as Social Security Numbers and credit-card data. Emails identified by [redacted] that contain PII are directed to the Pretty Good Privacy (PGP) system where they are securely stored for review or retrieval. The [redacted] console is monitored by the Information Security Officer's Security Operations team and personnel within the Information Assurance organization. Based on the nature of the alert generated from [redacted], the Privacy team will forward potential incidents to the USAID Cyber Security Incident Response Team for further analysis.

USAID provides an enterprise-wide approach for forensic investigations. This approach mitigates risks associated with forensics. An investigation begins when a Cyber Threat Analyst on the Information Assurance Computer Security Incident Response Team identifies a security incident that requires a forensic examination or receives a support request from an Authorized Requesting Office in USAID. There are six phases from 0-5, which includes, Pre-Investigation, Request, Incident Response, Acquisition, Analysis, and Presentation.

USAID utilizes multiple tools and mechanisms, such as FireEye, Network Intrusion Detection System, Department of Homeland Security's Einstein, and United States Computer Emergency Readiness Team (US-CERT) to monitor and detect malicious activities on USAID's network. Once a malicious activity has been identified, USAID uses EnCase Tool to take the snapshot of the infected machine and submits to US-CERT for analysis. US-CERT completes the analysis and notifies USAID with steps to resolve the issue. Typically, USAID will re-image the infected machine.

For digital rights management, USAID utilizes System Center Configuration Manager along with the ServiceNow Discovery tool to conduct software inventory on an annual basis. USAID does not have an automated process in place for license management; however, once USAID has identified all of the software, associated licenses are managed and monitored manually on a monthly basis. USAID starts the license renewal process 90 days in advance of expiration date. USAID is planning on implementing the ServiceNow Software Asset module to automate the license management process. For software that is not part of the standard deployment, the software will undergo the Software Request Process for approval. The Software Request Process includes review and approval from the Information Assurance, Engineering, and Operation departments.

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

Response:
Not applicable. USAID is using capabilities as described in clause (iii).

(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).

Response:

USAID has policies and procedures in place requiring entities, including contractors that provide services to USAID, to implement security management practices. USAID has documented policies and procedures in the *Automated Directive System (ADS) Chapter 545, Information Systems Security Policy*, dated March 9, 2016, to ensure that external entities have the required security controls. In addition, USAID requires external information systems not connected to USAID's AIDNet to comply with USAID's information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

USAID requires all connections from USAID's network to an information system outside of the system authorization boundary be documented with an interconnection security agreement. The interconnection security agreement documents the interface characteristics, security requirements, including the party responsible for each security requirement, and the nature of information communicated through the connection. The Chief Information Officer reviews the interconnection security agreements annually to ensure the security requirements are being appropriately maintained. Based on testing completed, USAID had several memorandums of understanding/interconnection security agreements that had expired.