Office of Inspector General

AUG 12 2016

The Honorable Constance Newman
U.S. African Development Foundation
President and Chief Executive Officer
1400 Eye Street NW
Suite 1000
Washington, DC 20005

Dear Ms. Newman:

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.

The U.S. Agency for International Development Office of Inspector General's (OIG) report on the U.S. African Development Foundation's (USADF) information systems is enclosed. While USADF 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 USADF's fiscal year 2016 Federal Information Security Modernization Act (FISMA)

compliance. Any deficiencies related to USADF's logical access policies, practices, or controls will be included in OIG's audit report on FISMA compliance later this year.

Please note that certain information contained in the attached material has been marked as "SBU" (sensitive but unclassified), meaning that public disclosure of this material could compromise the integrity of government computer systems and networks.

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.

Sincerely,

/s/

Ann Calvaresi Barr
Inspector General

Enclosure

CliftonLarsonAllen LLP
11710 Beltsville Drive, Suite 300
Calverton, Maryland 20705
301-931-2050 fax 301-931-1710
www.claconnect.com

July 26, 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 United States African Development Foundation (USADF). Enclosed are our responses.

In addressing the requirements, we leveraged the audit procedures performed during our current audit of USADF's compliance with the Federal Information Security Modernization Act of 2014 (FISMA). To address requirement that were not reviewed as part of the FISMA audit, we assessed 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 USADF 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 United States African Development Foundation (USADF) for the following selected covered systems: General Support System and the Department of Interior's Interior Business Center's Human Resources and Payroll systems.

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: USADF has documented logical access policies and procedures; however, the implementation of these polices needs strengthening. Specifically, USADF needs to configure password settings in accordance with the foundation's policy.

USADF's *Access Control Procedures (USADF Accounts Creation, Closures, and Review Procedures)*, last updated on April 11, 2014, details the process of how users are granted access, and how access is modified and removed. In addition, the *USADF Information Technology Security Implementation Plan*, dated March 12, 2015, covers access control procedures related to segregation of duties, least privilege, session lock, remote access, and controls over mobile devices.

USADF requires new users to fill out a system access form before gaining access to the General Support System. USADF grants access to its information systems based on a valid need-to-know by specified job duties and access approval. After creation of the new account, the user has three days to complete USADF's security awareness training. Rules of behavior are signed as a part of the training. Based on the testing completed, no weaknesses were identified related to new users competing initial security awareness training and signing rules of behavior.

User accounts are reviewed for inactivity every 30 days and are manually disabled or removed after 90 days of inactivity. When an account has been inactive for 90 days, the information technology (IT) supervisor emails the user's supervisor/manager to determine if the account is still needed. If the account is not needed, it is manually disabled from the system. Based on the testing completed, no weaknesses were identified related to access controls for inactive accounts.

~~(SBU)~~ Accounts on the General Support System are recertified [redacted] However, USADF has only one user in the Human Resource system and three users in the Payroll system, respectively. Therefore, the risk from not performing an annual recertification is minimal.

USADF requires separated/terminated users to complete an exit clearance form before leaving the organization. Based on testing completed, the only employee separated during the audit period completed the exit clearance form and their account was disabled timely.

USADF has configured its workstations to lock after 15 minutes of inactivity to reduce the likelihood of unauthorized access to the network. USADF has also configured its user accounts to lock after three unsuccessful login attempts. Based on testing performed, the parameter for password history in Active Directory was not configured in accordance with USADF policy. The current setting was 12 passwords remembered; however, USADF policy required the setting to be 24 passwords to be remembered. Upon notification of this issue to management, USADF revised the policy to 12 passwords remembered.

According to the *USADF Information Technology Security Implementation Plan*, the Information System Security Office or the Chief Information Officer must approve remote access before remote access is granted and users are required to sign a Telework Agreement Form. In addition, all methods of remote access are required to use two-factor authentication when connecting to the USADF network. USADF remote access users connect to the network using either a virtual private network or MyPC requiring a username, password and a token or MyPC requiring a username, password and a personal access code. USADF is in the process of converting all remote users to MyPC. Based on the testing completed, no weaknesses were identified related to access controls for remote access.

Mobile devices are allowed to access USADF information systems provided they are (1) approved, (2) scanned with the most current enterprise virus protection software and virus definitions, and (3) encrypted with USADF approved cryptographic mechanisms consistent with FIPS 140-2 *Security Requirements for Cryptographic Modules*. Based on the testing completed, no weaknesses were identified related to access controls for mobile devices.

(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.

~~(SBU)~~ **Response:** The *USADF Information Technology Security Implementation Plan* requires administrative rights to be based on "least privilege" and "need-to- know" principles. USADF grants privileged access to only two users. [redacted]

(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.

~~(SBU)~~ **Response:** [redacted] The organization plans to implement it by December 31, 2016.

(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: USADF uses Microsoft's Volume License Center to conduct inventories of the software on the USADF Network and USADF workstations. The results are documented on Microsoft's site for review at any time by the USADF IT supervisor.

(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.

~~(SBU)~~ **Response:** [redacted]

USADF has outsourced forensic and visibility investigative capabilities of threats entering or attempting to enter its network to the United States Computer Security Readiness Team (US-CERT). USADF has a memorandum of understanding (MOU) with the Department of Homeland Security and US-CERT that defines these capabilities.

USADF has the capability to conduct automated inventories by using the Microsoft Volume License Center for digital rights management. USADF has a contract with Microsoft that defines the capability of Microsoft to provide this software inventory list to USADF.

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

Response:

USADF has a weekly conference call with US-CERT to discuss any incidents that may have occurred. Per USADF's MOU with DHS and US-

CERT, the Office of Cybersecurity and Communications deploys and operates EINSTEIN cybersecurity capabilities on USADF's information systems to monitor network traffic indicating known or suspected malicious cyber activity. If an incident occurs, US-CERT investigates the incident and provides USADF a report that analyzes the incident and provides recommendations for remediation.

USADF has the capability to conduct automated inventories by using the Microsoft Volume License Center for digital rights management. The IT Supervisor can view the software inventory of licenses for USADF servers and workstations by logging into the Microsoft site.

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

~~(SBU)~~ **Response:** [redacted] USADF is one of 42 small and micro agencies identified in a task order awarded by the Department of Homeland Security under the Alliant Government-wide Acquisition Contract to receive Continuous Monitoring as a Service (CMaaS). This CMaaS provides continuous diagnostics monitoring tools to include data exfiltration/data loss prevention capabilities and, according to management, will be implemented within the next fiscal year.

(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: The *USADF Information Technology Security Implementation Plan* requires entities, including contractors that provide services to USADF to implement security management practices that adhere to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. In addition, non-USADF systems connections to the USADF network must be documented through an interconnection security agreement or processing agreement in the form of a MOU or Memorandum of Agreement (MOA).

USADF has access to the Federal Risk and Authorization Program's (FedRAMP) authorization to operate for Office 365 (dated April 19, 2016) and the associated security documentation, such as the system security plan, risk assessment, and the security assessment report. Office 365 is a FedRAMP compliant Software as a Service information system. In addition, USADF has contracts with Microsoft for Office 365 and with SmartSimple for the Program Support System which state that these contractor systems must adhere to NIST SP 800-53. USADF also has an MOU with the Department of Interior's Interior Business Center for the Human Resources and Payroll systems and an Interagency Agreement with the Department of Treasury Franchise Fund for the Travel, Oracle Financials, and PRISM systems. Both of these agreements state that their interconnections must

adhere to NIST SP 800-53 requirements. NIST SP 800-53, Revision 4, includes the following controls related to the information security practices described in subparagraph (D):

- CM-10: Software Usage Restrictions (software inventory and licensing /digital rights management capabilities).
- IR-7: Incident Response Assistance (forensics capabilities).
- IR-10: Integrated Information Security Analysis Team (forensics capabilities).
- SC-7 (10): Boundary Protection | Prevent Unauthorized Exfiltration (data exfiltration monitoring and detection, and data loss prevention capabilities).