Office of Inspector General

AUG 12 2016

The Honorable Dana Hyde
President and Chief Executive Officer
Millennium Challenge Corporation
1099 14th Street NW
Suite 700
Washington, DC 20005

Dear Ms. Hyde:

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 Millennium Challenge Corporation's (MCC) information systems is enclosed. While MCC 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 MCC's fiscal year 2016 Federal Information Security Modernization Act (FISMA) compliance. Any deficiencies related to MCC's logical access policies, practices, or controls will be included in OIG's audit report on FISMA compliance later this year.

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

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

August 9, 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 Millennium Challenge Corporation (MCC). Enclosed are our responses.

In addressing the requirements, we leveraged the audit procedures performed during our current audit of MCC'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 MCC 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 Millennium Challenge Corporation (MCC) for the following selected covered systems: MCC Network and MCC Management Information System (MCC MIS).

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:
MCC has documented logical access policies and procedures and has implemented the procedures for the covered systems. MCC's *Access Control Procedures* dated March 16, 2016, describes the process of how users are granted access, how access is modified and how access is removed. In addition, MCC's *Information System Security Policy,* dated October 30, 2015, covers access control procedures related to segregation of duties, least privilege, session lock, remote access, and controls over mobile devices.

MCC manages user access requests through the ServiceNow internal SharePoint site, which houses users' access request forms. Rules of behavior are signed as a part of the security awareness training required by MCC and tracked through the Learning Management System. User accounts are automatically disabled after 45 days of inactivity. The disabled accounts are then manually reviewed to see if the accounts have an exemption to the inactivity rule. Access enforcement is handled by requiring users to attend the security awareness training and information technology briefing before being allowed on the network. In addition, the Office of Domestic and International Security will verify that the individual requesting a new account has submitted their background investigation security package via the U.S. Office of Personnel Management's Questionnaire for Investigations Processing or will verify security clearances obtained from other Federal agencies. Users are also only granted the permissions, which were requested on their access request form.

MCC uses Varonis to monitor the network for changes in access and account creation. Varonis sends near real-time automated alerts when user accounts are locked out, user accounts are enabled, passwords are reset, privileged accounts are enabled, or permissions are changed on protected folders. The Chief Information Security Officer staff reviews alerts and removes the new access or disables the new account if it is unapproved. In addition, the security team reviews all network user accounts on a quarterly basis and reports the findings to appropriated parties. The process is captured within SharePoint.

Users requiring privileged access complete the administrative access request form, which is reviewed by the Chief Information Security Officer for approval. MCC policy requires administrator accounts to be created with the least amount of privilege needed to complete their assigned task. The policy also requires administrators to use different credentials to perform their administrative tasks.

MCC has configured its workstations to lock after 15 minutes of inactivity to reduce the likelihood of unauthorized access to the network. All users are granted remote access to the MCC Network and have the option of getting either a hardware token or a software token for multi-factor authentication.

MCC MIS inherits MCC Network's access control procedures unless otherwise noted in a waiver or exemption. Currently the only waiver in place is for inactive users to be disabled after 120 days instead of the MCC policy of 45 days.

Based on testing completed, MCC did not maintain exit checklists for a sample of terminated employees to ensure all MCC hardware is returned and access is properly terminated. However, no terminated users maintained their system access after termination.

In addition, based on the testing completed, MCC is following the access controls procedures for the MCC Network and MCC MIS systems.

(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:
MCC currently has logical access controls in place for privileged users. MCC 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 CISO.

Multi-factor authentication for privileged users is currently not implemented.

(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:
MCC has not fully implemented multi-factor authentication for privileged and non-privileged users. MCC uses the Department of State's (State's) Identity, Credentialing, and Access Management system. However, MCC's card issuing system cannot issue certificates on the contractor's card until the system is upgraded. Delays for the system upgrade have extended over a year while State completed an Authorization to Operate for the upgraded system. Therefore, MCC has to send its contractors to State to receive their certificates using the State System, but it is a slow process. MCC plans to implement the new system and implement multi-factor authentication for all users by the end of fiscal year 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:**
> MCC uses Microsoft's System Center Configuration Manager to conduct inventories of the software on the MCC Network. The results are documented on MCC's internal SharePoint site for review at any time by the Chief Information Officer/Chief Information Security Officer staff. MCC has a policy documented in the *Information System Security Policy*, dated October 30, 2015, to perform a software inventory on a quarterly basis. MCC also performs an annual reconciliation of all active licenses by comparing licenses purchased to licenses in use. If MCC is using more licenses than purchased, MCC will issue a contract modification to procure more licenses. If MCC is not using the full amount of licenses, MCC will modify the contract to purchase fewer licenses for the following year. For software that is not part of the standard deployment, such as Microsoft Project or Microsoft Visio, license checks are performed whenever the software install is requested.
>
> ***(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, MCC has the capability to scan all outgoing email via Office 365's data loss prevention solution to ensure no personally identifiable information leaves the MCC Network. In addition, MCC can monitor the network and determine whether there are rouge hosts or MCC employees that are exfiltrating data.
>
> Regarding forensic and visibility capabilities, MCC can investigate any threat entering or attempting to enter its network. In addition, MCC can monitor the network and determine whether there are rouge hosts connected to the network.
>
> For digital rights management, MCC has the capability to conduct automated inventories of the software on the MCC Network.
>
> ***(iii) A description of how the covered agency is using the capabilities described in clause (ii).***
>
> **Response:**
> For data loss prevention, MCC uses Office 365 to scan all outgoing email to ensure no personal data such as social security numbers or passport numbers leave the agency. Only encrypted personally identifiable information is allowed to pass through the Office 365 data loss prevention solution. MCC also uses Varonis to scan the network for personally identifiable information and detect anomalous behavior to prevent unauthorized access to the personally identifiable

information. In addition, MCC uses BRO Intrusion Detection System to monitor the network and determine whether there are rouge hosts or MCC employees that are exfiltrating data. If exfiltration is detected, a notification is sent to the Chief Information Officer/Chief Information Security Officer staff who will review the connection. If it is determined that the connection is unauthorized, the staff will terminate the connection. Once the connection is terminated, the Chief Information Officer/Chief Information Security Officer staff will open an investigation as well as report the incident to the United States Computer Emergency Readiness Team.

Regarding forensic capability, MCC has a dedicated team to research suspicious activity. Once the MCC team has positively identified an incident requiring forensic analysis, the team will use several tools for analysis, such as Bit 9, Suracata, Windows Event Log, Varonis, and Virus Total. If further analysis is needed, MCC will send the information to United States Computer Emergency Readiness Team who will perform further analysis on the suspicious file. MCC also correlates the newly identified incident using indicators of compromise. These indicators can be correlated to past incidents to look for patterns and help speed up the analysis process.

For digital rights management, MCC uses Microsoft's System Center Configuration Manager to conduct automated inventories of software installed on the MCC Network. The results are documented on MCC's internal SharePoint site for review at any time by the Chief Information Officer/Chief Information Security Officer staff. MCC has a policy documented in the *Information System Security Policy* to perform a software inventory on a quarterly basis. MCC also performs an annual reconciliation of all active licenses to compare licenses purchased to licensees in use. If MCC is using more licenses than purchased, MCC will issue a contract modification to procure more licenses. If MCC is not using the full amount of licenses, MCC will modify the contract to purchase fewer licenses for the following year. For software which is not part of the standard deployment, such as Microsoft Project or Microsoft Visio, license checks are performed whenever the software install is requested.

(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. MCC is using capabilities described in clause (ii).

(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
MCC has policies and procedures in place requiring entities, including contractors that provide services to MCC, to implement security management practices. MCC's *Information System Security Policy* requires non-MCC systems connections to MCC Network to be documented through an interconnection security agreement. The agreement identifies what security controls are required

to be in place and who is responsible for implementing the required security controls. In addition, MCC uses contractor-operated systems, such as Office 365, that do not have dedicated connections between them and MCC. MCC leverages and has access to the Federal Risk and Authorization Program's (FedRAMP) authorization to operate for Office 365 (dated November 13, 2014) 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.

MCC's *Background Investigations and Clearances (Security Clearances and Facility Access Clearances) for Federal Employment, Contract Service and/or Volunteer Service*, requires that every MCC contractor undergo a background investigation and that all incumbents in the same positions undergo regular reinvestigations. MCC's requirements are consistent with the Office of Personnel Management's guidelines for conducting background investigations and for determining eligibility for a facility clearance.

All personnel, including contractors or others working on behalf of MCC, accessing MCC systems are required to attend initial security awareness training and annual refresher training. In addition, contractors with system access must comply with the same access control procedure noted above.