OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2018 in Support of FISMA

AUDIT REPORT A-MCC-19-001-C
OCTOBER 24, 2018

1300 Pennsylvania Avenue NW • Washington, DC 20523
https://oig.usaid.gov • 202-712-1150

Office of Inspector General, U.S. Agency for International Development

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, U.S. African Development Foundation, Inter-American Foundation, Millennium Challenge Corporation, and Overseas Private Investment Corporation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: ig.hotline@usaid.gov
Complaint form: https://oig.usaid.gov/complainant-select
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: October 24, 2018

TO: MCC, Department of Administration and Finance, Vice President, Cynthia Huger

FROM: Deputy Assistant Inspector General for Audit, Alvin A. Brown /s/

SUBJECT: MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2018 in Support of FISMA (A-MCC-19-001-C)

Enclosed is the final audit report on the Millennium Challenge Corporation's (MCC) information security program for fiscal year 2018, as required by the Federal Information Security Modernization Act of 2014 (FISMA). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit. The contract required Clifton to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Clifton's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on MCC's compliance with FISMA. Clifton is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which Clifton did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether MCC implemented an effective information security program.[1] To answer the audit objective, Clifton tested MCC's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Clifton auditors reviewed four of the seven information systems in MCC's inventory dated December 2017. Fieldwork took place at MCC's headquarters in Washington, DC, from May 1 to August 27, 2018.

[1] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

The audit firm concluded that MCC generally implemented an effective information security program by implementing 66 of 74 selected security controls for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of the corporation's information and information systems. Among the controls MCC implemented were the following:

- An effective assessment and authorization process, including controls for planning, risk assessments, and security assessments and authorizations
- An enhanced account management process
- An effective contingency planning process
- An effective training program for information security awareness
- Effective identification and authentication processes

The audit firm also identified some deficiencies. For example, as summarized in the table below, Clifton noted weaknesses in eight controls, which fall into five of the eight FISMA metric domains.[2] These weaknesses increase MCC's information and information systems' vulnerability to unauthorized access, use, disclosure, disruption, modification, or destruction.

Fiscal Year 2018 IG FISMA Metric Domains	**Weaknesses Identified**
Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	X
Security Training	
Information Security Continuous Monitoring	
Incident Response	X
Contingency Planning	

To address the weaknesses identified in the report, we recommend that MCC take the following actions.

To enhance its enterprise risk management strategy, we recommend that MCC's chief risk officer:

Recommendation 1. Develop and implement its enterprise risk management program to include a strategy to manage risks associated with the operations and use of information systems.

[2] Each year inspectors general are required to complete metrics to independently assess their agencies' information security programs. The above metrics appear in "FY 2018 Inspector General Federal Information Security Modernization Act for 2014 (FISMA) Reporting Metrics," by the Office of Management and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency, May 24, 2018.

To improve privacy documentation, we recommend that MCC's chief information officer:

Recommendation 2. Update the privacy threshold analysis for the MCC management information system with the revised template to determine whether a privacy impact assessment is required.

To improve controls over background investigations, we recommend that MCC's Domestic and International Security Office:

Recommendation 3. Update MCC's "Background Investigation and Clearances for Federal Employment, Contract Service and/or Volunteer Service at the Millennium Challenge Corporation" policy to reflect the current personnel security controls.

Recommendation 4. Document and implement a process to review the data within the Background Investigation Access Database to validate whether the data are complete, accurate, and kept up-to-date.

Recommendation 5. Document and implement a process to track reinvestigations of employees and contractors and initiate reinvestigations in a timely manner.

In finalizing the report, Clifton evaluated MCC's responses to the recommendations. After reviewing that evaluation, we consider all five recommendations resolved but open pending completion of planned activities. For all five recommendations, please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance extended to our staff and Clifton employees during the engagement.

Audit of the Millennium Challenge Corporation's Compliance with the Federal Information Security Modernization Act of 2014

Fiscal Year 2018

Final Report

CliftonLarsonAllen LLP
901 N. Glebe Road, Suite 200
Arlington, VA 22203
571-227-9500 | fax 571-227-9552
CLAconnect.com

CliftonLarsonAllen LLP
901 N. Glebe Road, Suite 200
Arlington, VA 22203
571-227-9500 | fax 571-227-9552
CLAconnect.com

October 15, 2018

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:

CliftonLarsonAllen LLP is pleased to present our report on the Millennium Challenge Corporation's (MCC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA).

We appreciate the assistance we received from the staff of MCC and appreciate the opportunity to serve you. We will be pleased to discuss any questions you may have.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Inspector General
United States Agency for International Development

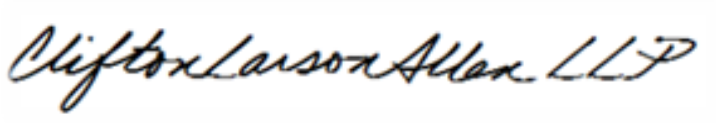
CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Millennium Challenge Corporation's (MCC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether MCC implemented an effective information security program. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls from four of MCC's seven information systems. Audit fieldwork was performed at the MCC's headquarters in Washington, D.C., from May 1, 2018 to August 27, 2018.

Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

We concluded that MCC generally implemented an effective information security program by implementing many of the selected security controls for selected information systems. Although MCC generally implemented an effective information security program, its implementation of a subset of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the corporation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in five out of the eight Inspector General (IG) FISMA Metric Domains and have made five recommendations to assist MCC in strengthening its information security program. In addition, findings related to recommendations from prior years were closed.

Additional information on our findings and recommendations are included in the accompanying report.



CliftonLarsonAllen LLP

Arlington, Virginia
October 15, 2018

TABLE OF CONTENTS

SUMMARY OF RESULTS

Background

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an annual evaluation of the Millennium Challenge Corporation's (MCC's) information security program. The objective of this performance audit was to determine whether MCC implemented an effective[2] information security program.

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget (OMB) and to congressional committees on the effectiveness of their information security program.

FISMA also requires agency Inspectors Generals (IGs) to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by the National Institute of Standards and Technology (NIST). In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

OMB and the U.S. Department of Homeland Security (DHS) provide annual instructions to Federal agencies and IGs on preparing FISMA reports. On October 16, 2017, OMB issued Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete metrics[3] to independently assess their agencies' information security programs.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] For this audit, an effective information security program is defined as implementing certain security controls for selected information systems in support of FISMA.

[3] The IG FISMA metrics will be completed as a separate deliverable.

The FY 2018 metrics are designed to assess the maturity[4] of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover, as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2018 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

For this audit, CLA reviewed selected[5] controls related to the metrics from four of MCC's seven information systems[6] in its FISMA inventory as of December 2017.

The audit was performed in accordance with generally accepted government auditing standards. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives.

Audit Results

CLA concluded that MCC generally implemented an effective information security program by implementing 66 of 74 selected security controls for selected information systems. For example, MCC:

- Maintained an effective assessment and authorization process, including controls around planning, risk assessments, and security assessment and authorization.
- Maintained and enhanced its account management process.
- Maintained an effective contingency planning process
- Maintained an effective whitelisting of software.
- Maintained an effective awareness training program.
- Maintained effective identification and authentication processes.

[4] The five levels in the maturity model are: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized.
[5] See Appendix III for a list of controls selected.
[6] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Although MCC generally implemented an effective information security program, its implementation of 8 of the 74 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the corporation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. As a result, CLA noted weaknesses in the following FISMA Metric Domains (Table 2) and made five recommendations to assist MCC in strengthening its information security program.

Table 2: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in the FY 2018 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains	Weaknesses Noted in FY 2018
Identify	**Risk Management**	MCC Needs to Better Document its Enterprise Risk Management Strategy **(Finding 1)**
Protect	**Configuration Management**	MCC Needs to Strengthen Configuration Management Controls (**Finding 5**)
	Identity and Access Management	MCC Needs to Strengthen Background Investigation Controls (**Finding 3**)
	Data Protection and Privacy	MCC Needs to Strengthen Privacy Impact Assessment Controls (**Finding 2**)
	Security Training	No weaknesses noted.
Detect	**Information Security Continuous Monitoring**	No weaknesses noted.
Respond	**Incident Response**	MCC Needs to Strengthen Incident Response Controls (**Finding 4**)
Recover	**Contingency Planning**	No weaknesses noted.

In response to the draft report, MCC outlined and described its plans to address all five audit recommendations. Based on our evaluation of management comments, we acknowledge management decisions on all recommendations. MCC's comments are included in their entirety in Appendix II. In addition, all five recommendations are resolved, but open pending completion of planned activities. The following section provides additional information on the findings identified.

AUDIT FINDINGS

1. MCC Needs to Better Document its Enterprise Risk Management Strategy

Cybersecurity Framework Domain: *Identify*
FY 18 FISMA IG Metric Area: *Risk Management*

NIST Special Publication 800-53, Revision 4, security control PM-9, states the following regarding risk management strategy:

> The organization:
> a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and
> b. Implements the risk management strategy consistently across the organization.

OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016), Section II, "Establishing Enterprise Risk Management In Management Practices," states the following:

> ERM [enterprise risk management] framework also includes the concepts of risk appetite, risk tolerance, and portfolio view:
> ……..
> - A portfolio view of risk-provides insight into all areas of organizational exposure to risk (such as reputational, programmatic performance, financial, information technology, acquisitions, human capital, etc.), thus increasing an Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment.

MCC needs to better document its strategy to manage risks associated with the operation and use of information systems implementation as a part of its Enterprise Risk Management (ERM) Program. MCC had not yet documented a comprehensive ERM Program and Strategy. In response to OMB Circular No. A-123, MCC developed a Governance Structure, Risk Profile, and a Risk Assessment Framework Tool. However, MCC had not yet developed the ERM Program to provide insight into all critical areas of organizational risk to the Corporation, including information security.

Without a comprehensive ERM Program, MCC will not be able to properly assess risk across the organization, resulting in a greater chance of experiencing unanticipated outcomes as changes in the environment occurs. Therefore, CLA is making the following recommendation.

Recommendation 1: *The Millennium Challenge Corporation's Chief Risk Officer should develop and implement its Enterprise Risk Management program to include a strategy to manage risks associated with the operation and use of information systems*.

2. MCC Needs to Strengthen Privacy Impact Assessment Controls

Cybersecurity Framework Domain: *Protect*
FY 18 FISMA IG Metric Area: *Data Protection and Privacy*

NIST Special Publication 800-53, Revision 4, security control AR-2, states the following regarding privacy impact assessments:

> The organization:
> a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
> b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

The *MCC Privacy Policy*, states the following regarding PIAs:

> System Owners must:
> a. Conduct Privacy Impacts Assessments of the systems every three years or when a major change occurs;
> b. Have all Privacy Impact Assessments approved by the Chief Privacy Officer (CPO); and
> c. Revalidate Privacy Impact Assessments annually.

The *MCC Privacy Threshold Analysis* defines Privacy Threshold Analysis (PTA) within the PIA forms as a "Methodology that provides information technology (IT) security professionals with a process for assessing whether a PIA is necessary."

MCC did not adequately complete and review the PTA for 1 of the 4 systems selected. Specifically, the PTA for the MCC Management Information System contained conflicting information about whether or not the system contained Personally Identifiable Information (PII).

For example, we noted that the PTA form contained the following conflicting information about whether the system contained PII.

- A check-box was checked "No" in response to the following, "Does the technology, system, or program collect, maintain, and/or share information that relates to an individual (i.e. birthdates, passport number, social security number (SSN), biometric…"

- The form contained comments in the privacy officer/reviewer comments section that stated the following, "The system contains PII, obtained from the security clearance and background check documents, and stores it in the system. The system owner should conduct a Privacy Impact Assessment to determine the risk to the sensitive information while stored within the system."

Additionally, the PTA form contained conflicting statements in the Designation field. Specifically, we noted the following conflicting statements in the PTA:

- "This is not a Privacy Sensitive Project/System. A Privacy Impact Assessment (PIA) is not required at this time as this project/system does not collect or retain any Personally Identifiable Information."
- "This is a Privacy Sensitive Project/System. Personally Identifiable Information (PII) is captured or retained; the MCC Project/Office/Mission Lead should proceed to reviewing and completing the MCC PIA Process and Procedure."

As such, the PTA form had conflicting responses mistakenly entered and not corrected during the review process. Therefore, it was not clear whether a PIA was required. Upon notification of the issue, MCC updated the template used for PTAs to clearly state whether a PIA is required and whether the system maintains PII.

Without the proper completion of PTAs, MCC will not be fully aware of all privacy related systems that contain PII, thus increasing the risk that effective security controls are not in place for those systems. Therefore, CLA is making the following recommendation.

> ***Recommendation 2:*** *The Millennium Challenge Corporation's Chief Information Officer should update the privacy threshold analysis for the MCC Management Information System with the revised template to determine whether a privacy impact assessment is required.*

3. MCC Needs to Strengthen Background Investigation Controls

Cybersecurity Framework Domain: *Protect*
FY 18 FISMA IG Metric Area: *Identity and Access Management*

NIST Special Publication 800-53, Revision 4, security control PS-1, states the following regarding personnel security:

> The organization:
> a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
> 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
> b. Reviews and updates the current:
> 1. Personnel security policy [Assignment: organization-defined frequency]; and

2. Personnel security procedures [*Assignment: organization-defined frequency*].

In addition, security control PS-3, states the following regarding personnel security:

> The organization:
> …
> b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

MCC's background investigations processes need to be strengthened. Specifically, CLA noted the following weaknesses with MCC's background investigation policy and procedures, tracking and timelines.

Background Investigation Policy and Procedures

The MCC *Background Investigation and Clearances for Federal Employment, Contract Service and/or Volunteer Service at the Millennium Challenge Corporation* policy had not been reviewed or updated since June 11, 2013, and was no longer reflective of MCC's current processes. Management did not have a process in place to review the policy periodically or when there was a major change to the process. MCC was in the process of updating the policy for background investigations; however, it had not yet been approved or implemented.

Background Investigations Tracking

MCC did not effectively track background investigations. MCC uses a Background Investigation Access Database tool to track background investigation data; however, the data within the database was not always complete and accurate. Based on a review of 48 employees from the total population of 286 employees and contractors with secret and top secret clearances:

- 5 reinvestigation start dates were not tracked;
- 10 clearances were not updated to reflect the current clearance held by the individual; and
- 1 reinvestigation date was not updated to reflect that the reinvestigation has been completed.

MCC did not have a consistent process in place to ensure that the Background Investigation Access Database was up-to-date with complete and accurate data. MCC manually updated the Database, which made it prone to human error considering the ever-changing data. For example, management indicated that the background investigation status can be in flux depending on when position designations are received by Human Resources, as well as the Department of State stopping and re-starting the processing of background investigations.

Background Investigation Timeliness

Executive Order 12968, *Access to Classified Information* and the *Investigative Standards for Background Investigations for Access to Classified Information*[7] states the following regarding Access Level and Reinvestigation Timeframes:

Access Level	Required Investigation
Top Secret	Reinvestigation every 5 years
Secret	Reinvestigations every 10 years

MCC did not perform timely background investigations. Specifically:

- 13 out of 114 individuals with Top Secret clearances were not reinvestigated within the five years, as required; and
- 2 out of 172 individuals with Secret clearances were not reinvestigated within 10 years, as required.

Background Investigation and Clearances for Federal Employment, Contract Service and/or Volunteer Service at the Millennium Challenge Corporation policy did not include requirements detailing the frequency in which individuals should be reinvestigated. The lack of reinvestigation requirements and the failure to adequately track background investigation data has led to delayed reinvestigations of individuals with access to sensitive information.

Without an up-to-date background investigation policy, MCC's personnel security controls may not be implemented consistently. In addition, without complete and accurate tracking of employee investigations, employees may not be investigated timely or sufficiently for their job responsibilities. This may result in unauthorized individuals gaining access to sensitive information. Therefore, CLA is making the following recommendations.

> ***Recommendation 3:*** *The Millennium Challenge Corporation Domestic and International Security Office should update the* Background Investigation and Clearances for Federal Employment, Contract Service and/or Volunteer Service at the Millennium Challenge Corporation *to reflect the current personnel security controls.*
>
> ***Recommendation 4:*** *The Millennium Challenge Corporation Domestic and International Security Office should document and implement a process to review the data within the Background Investigation Access Database to validate whether the data are complete, accurate, and kept up-to-date.*
>
> ***Recommendation 5:*** *The Millennium Challenge Corporation Domestic and International Security Office should document and implement a process to track reinvestigations of employees and contractors and initiate reinvestigations in a timely manner.*

[7] https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/1997/fin-97-02/.

4. MCC Needs to Strengthen Incident Response Controls

Cybersecurity Framework Domain: *Respond*
FY 18 FISMA IG Metric Area: *Incident Response*

NIST Special Publication 800-53, Revision 4, security control IR-6, states the following regarding incident reporting:

> The organization:
> a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period].

In addition, *United States Computer Emergency Readiness Team (US-CERT) Reporting Guidelines*, states the following regarding incident notification:

> Agencies must report information security incidents, where the confidentiality, integrity, or availability of a federal information system of a civilian, Executive Branch agency is potentially compromised, to the NCCIC/US-CERT with the required data elements, as well as any other available information, within one hour of being identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department.

MCC did not formally track whether incidents were submitted to US-CERT in a timely manner. This occurred because MCC did not record the identification dates and time of incidents after analysis, and before submitting to US-CERT. Instead, MCC relied on its Security Operations Center to report timely to US-CERT after its analyses were completed. Therefore, we could not ascertain whether incidents were reported to US-CERT timely in accordance with *MCC's Incident Handling and Response Procedures* and US-CERT requirements.

Without an adequate record of timeframes for incident reporting, MCC cannot formally track whether incidents are reported timely to US-CERT. Upon notification of the issue, MCC took action to correct this weakness. Therefore, CLA is not making a recommendation at this time.

5. MCC Needs to Strengthen Configuration Management Controls

Cybersecurity Framework Domain: *Protect*
FY 18 FISMA IG Metric Area: *Configuration Management*

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control CM-3, states the following regarding configuration change control:

> The organization:
> ...
> b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.
> c. Documents configuration change decisions associated with the information system
> d. Implements approved configuration-controlled changes to the information system.

In addition, security control CM-4 states the following regarding security impact analysis, "the organization analyzes changes to the information system to determine potential security impacts prior to change implementation."

Additionally, the *MCC Configuration Management Procedure* requires the Chief Information Security Officer (CISO) team to review the security impact of the change request (CR).

Furthermore, Section 4. "Change Request (CR) Workflow" of the *MCC Configuration Management Procedure* states:

> All changes are initiated by the submission of a CR to the MCC Change Control Board (CCB). Changes are submitted via an online submission process and are tracked from initiation through closure by the CCB. Changes may be initiated by authorized user using the Change Request (CR) form.

Configuration management weaknesses were identified for one of the four sampled systems. Specifically, for a sample of 23[8] changes from the population of 244 closed change requests for the fiscal year (FY) 2018:

- No security impact analysis was completed for 8 changes.
- No change request forms were maintained for 8 changes.

To address a prior year FISMA audit recommendation,[9] MCC updated the *MCC Configuration Management Procedure* to require a security impact analysis to be completed for change requests. Additionally, MCC implemented ServiceNow[10] to manage and track change requests. The instances in which exceptions were noted occurred before MCC closed the audit recommendation and implemented the new policy and ServiceNow. Since MCC took corrective action to remediate this finding, CLA is not making a recommendation at this time.

[8] A sample of changes was selected for changes occurring between October 1, 2017, and May 8, 2018.

[9] Recommendation 5, *The Millennium Challenge Corporation Implemented Controls in Support of FISMA for Fiscal Year 2017, but Improvements Are Needed* (Audit Report No. A-MCC-17-006-C, September 28, 2017).

[10] ServiceNow is a commercial of the shelf product that provides a systematic approach to control the life cycle of all changes.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the Millennium Challenge Corporation (MCC) outlined its plans to address all five recommendations. MCC's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge management decisions on all five recommendations. Further, all five recommendations are resolved, but open pending completion of planned activities.

SCOPE AND METHODOLOGY

Scope

CLA conducted this audit in accordance with performance auditing standards, as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective. The audit was designed to determine whether MCC implemented certain security controls for selected information systems[11] in support of the Federal Information Security Modernization Act of 2014 (FISMA).

The audit included tests of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. CLA assessed MCC's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Personnel Security
- Planning
- Privacy
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Service Acquisition

For this audit, selected controls related to the FY2018 IG FISMA reporting metrics from four of MCC's seven information systems in MCC's systems inventory as of December 2017 were reviewed.

See Appendix III for a listing of selected controls. The audit also included a follow up on prior audit recommendations[12] to determine if MCC made progress in implementing the recommended improvements concerning its information security program.

[11] See Appendix III for a list of controls selected.

[12] *The Millennium Challenge Corporation Implemented Controls in Support of FISMA for Fiscal Year 2017, but Improvements Are Needed* (Audit Report No. A-MCC-17-006-C, September 28, 2017); *The Millennium Challenge Corporation Has Implemented Many Controls in Support of FISMA, but Improvements Are Needed* (Audit Report No. A-MCC-17-003-C, November 7, 2016); and *Audit of the Millennium Challenge Corporation's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, As Amended* (Audit Report No. A-MCC-16-001-P, October 26, 2015).

The audit fieldwork was performed at MCC's headquarters in Washington, D.C., from May 1, 2018 to August 27, 2018.

Methodology

To determine if MCC implemented an effective information security program, CLA conducted interviews with MCC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. Also, documents supporting the information security program were reviewed. These documents included, but were not limited to, MCC's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; and (5) change control documentation. Where appropriate, we compared documents, such as MCC's information technology policies and procedures, to requirements stipulated in National Institute of Standards and Technology special publications. In addition, tests of system processes were performed to determine the adequacy and effectiveness of those controls. Also, the status of FISMA audit recommendations for fiscal years 2015, 2016, and 2017[13] were reviewed.

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk, and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population. However, in cases where the entire audit population was not selected, the results cannot be projected and if projected may be misleading.

[13] Ibid. footnote 12.

Management Comments

MILLENNIUM CHALLENGE CORPORATION
UNITED STATES OF AMERICA

Memorandum

Millennium Challenge Corporation

DATE: October 01, 2018

TO: Mr. Mark Norman
Director, Information Technology Audit Division
Office of Inspector General
United States Agency for International Development Millennium Challenge Corporation

FROM: Cynthia Huger /s/
Vice President and Chief Financial Officer
Department of Administration and Finance
Millennium Challenge Corporation

SUBJECT: MCC's Response to the Draft Audit Report on the *Audit of the Millennium Challenge Corporation's Fiscal Year 2018 Compliance with the Federal Information Security Management Act of 2014, As Amended* Draft Report No. A-MCC-18-00X-C, dated September 24, 2018

Millennium Challenge Corporation (MCC) appreciates the opportunity to comment on the Fiscal Year 2018 audit of MCC's compliance with the regulatory requirements of the Federal Information Security Modernization Act of 2014, as amended (FISMA) and considers your role vital in helping to achieve and sustain our FISMA compliance.

Our Management Response to your recommendations follows:

To enhance its enterprise risk management strategy, we recommend that MCC's chief risk officer:

Recommendation 1. Develop and implement its enterprise risk management program to include a strategy to manage risks associated with the operations and use of information systems.

MCC Management Response: MCC concurs with this recommendation. MCC's chief risk officer will ensure that its MCC Integrated Risk Management Framework document (which will include documentation of the implementation of its Enterprise Risk Management program) includes its strategy to manage risks associated with the operation and use of information systems by June 30, 2019.

To improve privacy documentation, we recommend that MCC's chief information officer:

Recommendation 2. Update the privacy threshold analysis for the MCC management information system with the revised template to determine whether a privacy impact assessment is required.

MCC Management Response: MCC concurs with this recommendation. MCC's chief information officer will update its procedures and privacy threshold template to ensure clarity in its privacy impact assessment by November 30, 2018.

To improve controls over background investigations, we recommend that MCC's Domestic and International Security Office:

Recommendation 3. Update its "Background Investigation and Clearances for Federal Employment, Contract Service and/or Volunteer Service at the Millennium Challenge Corporation" to reflect the current personnel security controls.

MCC Management Response: MCC concurs with this recommendation. MCC's Domestic & International Security Office will provide the Personnel Security Policy which includes the Background Investigation and Clearances for Federal Employment, Contract Service and/or Volunteer Service by December 31, 2018.

Recommendation 4. Document and implement a process to review the data within the existing Access –based Security Database to validate whether the data are complete, accurate, and kept up-to-date.

MCC Management Response: MCC concurs with this recommendation. MCC Domestic & International Security will document and implement a manual process that validates the completeness and accuracy of the existing Access-based Security Database with a long-term goal of implementing a system to perform the process. MCC will provide a formal management decision no later than March 29, 2019.

Recommendation 5. Document and implement a process to track reinvestigations of employees and contractors and initiate reinvestigations in a timely manner.

MCC Management Response: MCC concurs with this recommendation. MCC Domestic & International Security will document and implement a manual process that tracks reinvestigation of employees and contractors in a timely manner with a long-term goal of implementing a system to perform the process. MCC will provide a formal management decision no later than March 29, 2019.

CC: IG/MCC, Alvin Brown
IG/MCC, Lisa Banks
IG/MCC, Aleta Johnson
MCC/A&F/CIO, Vincent Groh
MCC/A&F/DIS, Douglas Fairfield
MCC/A&F/CRO, Alice Miller
MCC/A&F/Senior Director, Chris Ice
MCC/A&F/ARC, Jude Koval
MCC/A&F/CISO, Miguel Adams

Summary of Controls Reviewed

The following table identifies the controls selected for testing.

Control	Control Name	Number of Systems Tested
AC-1	Access Control Policy and Procedures	1
AC-2	Account Management	1
AC-8	System Use Notification	2
AC-17	Remote Access	2
AR-1	Governance and Privacy Program	1
AR-2	Privacy Impact and Risk Assessment	4
AT-1	Security Awareness and Training Policy and Procedures	1
AT-2	Security Awareness Training	1
AT-3	Role-Based Security Training	1
AT-4	Security Training Records	1
CA-1	Security Assessment and Authorization Policies and Procedures	1
CA-2	Security Assessments	2
CA-3	System Interconnections	1
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	3
CA-7	Continuous Monitoring	1
CM-1	Configuration Management Policy and Procedures	1
CM-2	Baseline Configuration	2
CM-3	Configuration Change Control	1
CM-6	Configuration Settings	1
CM-7	Least Functionality	1
CM-8	Information System Component Inventory	2
CM-9	Configuration Management Plan	2
CM-10	Software Usage Restrictions	1
CP-1	Contingency Planning Policy and Procedures	1
CP-2	Contingency Plan	1
CP-3	Contingency Training	1
CP-4	Contingency Plan Testing	1
CP-6	Alternate Storage Site	1
CP-7	Alternate Processing Site	1
CP-8	Telecommunications Services	1
CP-9	Information System Backup	1
IA-1	Identification and Authentication Policy and Procedures	1
IA-3	Device Identification and Authentication	1
IR-1	Incident Response Policy and Procedures	1
IR-4	Incident Handling	1

Control	Control Name	Number of Systems Tested
IR-6	Incident Reporting	1
PL-2	System Security Plan	3
PL-4	Rules of Behavior	1
PL-8	Information Security Architecture	1
PM-5	Information System Inventory	1
PM-7	Enterprise Architecture	1
PM-8	Critical Infrastructure Plan	1
PM-9	Risk Management Strategy	1
PM-11	Mission/Business Process Definition	1
PM-12	Insider Threat Program	1
PS-1	Personnel Security Policy and Procedures	1
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	3
SA-3	System Development Life Cycle	1
SA-4	Acquisition Process	2
SA-8	Security Engineering Principles	1
SC-12	Cryptographic Key Establishment and Management	1
SI-2	Flaw Remediation	1
SI-4	Information System Monitoring	1