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

MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA

AUDIT REPORT A-MCC-20-001-C
NOVEMBER 12, 2019

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

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, Millennium Challenge Corporation, U.S. African Development Foundation, Inter-American Foundation, 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: November 12, 2019

TO: MCC, Co-Acting Vice President and Deputy Chief Financial Officer, Department of Administration and Finance, Adam J. Bethon

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

SUBJECT: MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA (A-MCC-20-001-C)

Enclosed is the final audit report on the Millennium Challenge Corporation's (MCC's) information security program for fiscal year 2019, 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 of RMA Associates, LLC (RMA), to conduct the audit. The contract required RMA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed RMA'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. RMA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which RMA 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, RMA 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." RMA auditors reviewed four of the seven information systems in MCC's

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

inventory dated October 2018. Fieldwork took place at MCC's headquarters in Washington, DC, from May 28 to September 16, 2019. It covered the period from October 1, 2018, through September 16, 2019.

The audit firm concluded that MCC generally implemented an effective information security program by implementing 85 of 101 instances of 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 those controls, MCC maintained:

- Security plans that explicitly define the authorization boundary for their systems;
- A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- An effective process for assessing risk associated with positions involving information system duties;
- An effective procedure to continuously monitor the network for unauthorized software;
- An effective security awareness training program that includes role-based training for positions with elevated information system permissions; and
- An accurate inventory of hardware and software assets.

The audit firm also identified some weaknesses. As summarized in the table below, RMA noted weaknesses in all eight FISMA metric domains. The weaknesses were mostly due to policy and procedures not being reviewed and updated in a timely manner, but weaknesses were also identified with MCC's contingency plans. With these weaknesses, MCC's information and information systems are potentially exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

Fiscal Year 2019 IG FISMA Metric Domains[2]	**Weaknesses Identified**
Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	X
Security Training	X
Information Security Continuous Monitoring	X
Incident Response	X
Contingency Planning	X

[2] The Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," April 9, 2019.

To address the weaknesses identified in RMA's report, we recommend that MCC's chief information officer take the following actions.

Recommendation 1. Create a monitoring plan to review and update policy, procedures, and agreements in accordance with the timeliness requirements established in agency policies.

Recommendation 2. Revise the contingency plan to accurately identify the alternate processing site and associated procedures.

Recommendation 3. In consultation with business owners, determine what information systems need to be prioritized for recovery; then, update the business process analysis and contingency plan to reflect these priorities.

Recommendation 4. Develop a procedure for contingency situations that defines the information technology personnel, their roles, responsibilities, authorities, and timeline for the contingency training personnel will receive upon assuming those roles.

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

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

RMA | Associates

Auditors. Consultants. Advisors.

Millennium Challenge Corporation (MCC)
Federal Information Security Modernization Act (FISMA) Audit

Final Report

Fiscal Year 2019

RMA | Associates
Auditors. Consultants. Advisors.

October 22, 2019

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:

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

Thank you for the opportunity to serve your organization and the assistance provided by your staff and that of MCC. We will be happy to answer any questions you may have concerning the report.

Respectfully,

Reza Mahbod

Reza Mahbod, CPA, CISA, CGFM, CICA, CGMA, CDFM
President
RMA Associates, LLC

RMA | Associates
Auditors. Consultants. Advisors.

Inspector General
United States Agency for International Development

October 22, 2019

RMA Associates, LLC (RMA) 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 the 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 MCC's headquarters in Washington, D.C., from May 28 to September 16, 2019.

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 objective.

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 agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in all eight Inspector General (IG) FISMA Metric Domains mostly due to policy and procedures not being reviewed within the organization-defined frequency. We made four 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.

Respectfully,

RMA Associates

RMA Associates, LLC

TABLE OF CONTENTS

SUMMARY OF RESULTS

Background

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) engaged RMA Associates, LLC, (RMA) 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 also 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. Because MCC is a federal agency, it is required to comply with federal information security requirements.

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.

Annually, OMB and the Department of Homeland Security (DHS) provide instructions to Federal agencies and IGs for assessing agency information security programs. On October 25, 2018, OMB issued OMB Memorandum 19-02, "Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements." According to this 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 fiscal year (FY) 2019 IG metrics are designed to assess the maturity[4] of an information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), Version 1.1: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2019 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, we reviewed selected[5] controls related to the metrics from four of seven information systems[6] in MCC's FISMA inventory as of October 2018.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

The audit concluded that MCC generally implemented an effective information security program by implementing 85 of 101[7] instances of selected security controls for selected information systems. For example, MCC maintained:

- Security plans that explicitly define the authorization boundary for their systems;
- A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- An effective process for assessing risk associated with positions involving information system duties;

[4] The five maturity models include: 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 systems and 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.

[7] There were 67 different NIST SP 800-53, Rev. 4 controls identified in the FY 2019 FISMA IG metrics. We tested only the 66 that were applicable to moderate and low impact systems. However, a control was counted for each system it was tested against. Thus, there were 101 instances of testing a control.

- An effective procedure to continuously monitor the network for unauthorized software;

- An effective security awareness training program that includes role-based training for positions with elevated information system permissions; and

- An accurate inventory of hardware and software assets.

Although MCC generally implemented an effective information security program, its implementation of 16 of 101 instances of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the corporation's information and information systems. As a result, we noted deficiencies in all eight IG FISMA Metric Domains (Table 2) and presented recommendations to assist MCC in strengthening its information security program.

Table 2: Cybersecurity Framework Security Functions mapped to deficiencies noted in FY 2019 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains	Deficiencies Noted in FY 2019
Identify	**Risk Management**	MCC needs to consistently review policy, procedures, and agreements periodically. (**Finding 1**)
Protect	**Configuration Management**	MCC needs to consistently review policy, procedures, and agreements periodically. (**Finding 1**)
	Identity and Access Management	MCC needs to consistently review policy, procedures, and agreements periodically. (**Finding 1**)
	Data Protection and Privacy	MCC needs to consistently review policy, procedures, and agreements periodically. (**Finding 1**)
	Security Training	MCC needs to consistently review policy, procedures, and agreements periodically. (**Finding 1**)
Detect	**Information Security Continuous Monitoring**	MCC needs to consistently review policy, procedures, and agreements periodically. (**Finding 1**)
Respond	**Incident Response**	MCC needs to consistently review policy, procedures, and agreements periodically. (**Finding 1**)
Recover	**Contingency Planning**	MCC needs to consistently review policy, procedures, and agreements periodically. (**Finding 1**) MCC needs to identify the alternate processing site. (**Finding 2**) MCC needs to identify priority information systems required for business processes. (**Finding 3**) MCC needs to define procedures for identifying individuals assuming IT contingency roles and for completing contingency training. (**Finding 4**)

The following section provides detailed findings.

AUDIT FINDINGS

1. MCC Needs to Consistently Review Policy, Procedures, and Agreements Periodically.

Cybersecurity Framework Domain: *All Domains*
FY 19 FISMA IG Metric Area: *All Functional Areas*

MCC's policy, procedures, and agreements were not always periodically reviewed to ensure they address current information security standards. The organization's requirement to review policy and procedure is every two years. During our inspection, we found five of MCC's 32 directives had not been reviewed and updated for at least two years. Specifically, as of August 14, 2019, MCC had not reviewed its:

- "National Cyber Security Division Service Level Agreement"[8] in 7 years, 5 months.
- "MCC Information System Security Policy" in 3 years, 9 months.
- "MCC Privacy Policy" in 3 years, 6 months.
- "Vulnerability Patch Management Desktop Guide" in 3 years, 6 months.
- System Security Plan supporting a general support system in 2 years, 5 months.

National Institute of Science and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, has 17 controls specifically addressing policies and procedures. The first control of each control family specifies that the organization reviews and updates the current policy and procedures in an Assignment: organization-defined frequency:

> a. Reviews and updates the current:
> 1. Control policy [*Assignment: organization-defined frequency*]; and
> 2. Control procedures [*Assignment: organization-defined frequency*].

MCC's *Policy on Creating and Maintaining MCC Policies* states:

> The default review period for any Policy is two years from the date of issuance. Any current Policy not including a review date should be reviewed no later than two years after its date of issuance.

There is no monitoring plan in place to review policy, procedures, and agreements to help ensure compliance with MCC's two-year review requirement. Therefore, the CIO may have overlooked reviewing the policies, procedures, and agreements to determine whether they have deviated from current control practices, and updating them as needed.

Over time, an agency's security practices may deviate from its written policies and procedures. There is also an increased risk that security practices will become unclear, misunderstood, and improperly implemented.

[8] This agreement contains procedures, such as what an organization must do and how they will do it.

Recommendation 1: We recommend that the Millennium Challenge Corporation's Chief Information Officer create a monitoring plan to review and update policies, procedures, and agreements in accordance with the timeliness requirements established in agency policies.

2. MCC Needs to Identify the Alternate Processing Site.

Cybersecurity Framework Domain: *Recover*
FY 19 FISMA IG Metric Area: *Contingency Planning*

MCC's depiction of the alternate processing site and associated procedures is not clearly stated in its contingency plan. The contingency plan states that one location has been deemed the interim recovery site to support the midrange disaster recovery configuration for MCC. Instead, it should have identified a different location as the alternate processing site.

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4 requires that an organization develop a Contingency Plan with alternate processing site arrangements. *NIST SP 800-53 Rev. 4* states:

> **CP-7 – ALTERNATE PROCESSING SITE**
>
> Control: The organization:
>
> *a.* Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;
>
> b. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

Although we could not determine the root cause, MCC did not update the contingency plan and the associated recovery procedures when it migrated to the system that is used for alternate processing purposes.

Without a clear description of the alternate site, the organization is at an increased risk that the contingency plan may be misunderstood and improperly implemented.

Recommendation 2: We recommend that the Millennium Challenge Corporation's Chief Information Officer revise its contingency plan to accurately identify the alternate processing site and associated recovery procedures.

3. MCC Needs to Identify Priority Information Systems Required for Business Processes.

Cybersecurity Framework Domain: *Recover*
FY 19 FISMA IG Metric Area: *Contingency Planning*

The information systems that are identified in the contingency plan for priority restoration do not fully support MCC's mission essential functions (MEFs). The MEFs are critical business processes that MCC executes day-to-day to accomplish its mission. The contingency plan identifies seven priority systems to recover in the event of a contingency. However, the business process analysis identifies eight as systems required to fulfill the MEFs and only two of those system names are identified in the contingency plan.

The *National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4* requires that an organization develop a contingency plan that establishes restoration priorities and is consistent with business functions and states:

> **CP-2 – CONTINGENCY PLAN**
>
> Control: The organization:
> a. Develops a contingency plan for the information system that:
>   1. Identifies essential missions and business functions and associated contingency requirements;
>   2. Provides recovery objectives, restoration priorities, and metrics; and
>   3. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.
>
> Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions.

MCC did not properly review information system requirements with business process owners when developing the contingency plan or prioritize the restoration of those systems. As a result, MCC may not be able to perform its MEFs if the information systems required to fulfill those MEFs are not appropriately prioritized for recovery.

Recommendation 3: We recommend that, in consultation with business owners, the Millennium Challenge Corporation's Chief Information Officer determine what information systems need to be prioritized for recovery; then, update the business process analysis and contingency plan to reflect these priorities.

4. MCC Needs to Define Procedures for Identifying Individuals Assuming IT Contingency Roles and for Completing Contingency Training.

Cybersecurity Framework Domain: *Recover*
FY 19 FISMA IG Metric Area: *Contingency Planning*

MCC does not have a procedure for contingency situations that identifies IT staff, including alternates, by role, name, responsibility, and authority. In addition, MCC does not have a procedure for individuals to complete contingency training within a specific time period of assuming contingency roles.

The *National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4* requires that an organization train to the Contingency Plan and states:

> **CP-3 – CONTINGENCY PLAN TESTING**
>
> Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:
> a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;
> b. When required by information system changes; and
> c. [Assignment: organization-defined frequency] thereafter.
>
> Supplemental Guidance: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training.

Although we could not determine the root cause, MCC IT personnel in contingency roles may not be able to fulfill contingency duties without training administered to them in a timely manner. As a result, MCC may not be able to adequately respond in a contingency situation.

Recommendation 4: We recommend that the Millennium Challenge Corporation's Chief Information Officer develop a procedure for contingency situations that defines the information technology personnel, their roles, responsibilities, and authorities; and the timeline for the contingency training they will receive upon assuming those roles.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, MCC outlined its plans to address all four 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 four recommendations. Further, all four recommendations are resolved, but open pending completion of planned activities.

SCOPE AND METHODOLOGY

Scope

RMA conducted this audit in accordance with Generally Accepted Government Auditing Standards, as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether MCC implemented certain security controls for selected information systems[9] 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 the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. We assessed MCC's performance and compliance with FISMA in the following areas:

- Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Awareness Training
- Information System Continuous Monitoring
- Incident Response
- Contingency Planning

For this audit, we reviewed selected controls related to the FY2019 IG FISMA Reporting Metrics from four of seven information systems in MCC's FISMA inventory as of October 2018.

The audit also included a follow up on prior audit recommendations[10] to determine if MCC made progress in implementing the recommended improvements concerning its information security program.

The audit fieldwork was performed at MCC's headquarters in Washington, D.C., from May 28 to September 16, 2019. It covered the period from October 1, 2018, through September 16, 2019.

[9] See Appendix III for a list of systems and controls selected.

[10] *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2018 in Support of FISMA* (Audit Report No. A-MCC-19-001-C, October 24, 2018).

Methodology

To determine if MCC implemented an effective information security program, we conducted interviews with MCC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. Additionally, we reviewed documentation supporting the information security program. These documents included, but were not limited to, MCC's (1) risk management policy; (2) configuration management procedures; (3) identity and access control measures; (4) security awareness training; and (5) continuous monitoring controls. We compared documentation against requirements stipulated in NIST special publications. Also, we performed tests of information system controls to determine the effectiveness of those controls, including a vulnerability assessment of MCC's network. Furthermore, we reviewed the status of FISMA audit recommendations from FY 2018.

In testing the effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk and the significance of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the proportion of deficient items found compared to the total population available for review when documenting the results of our testing. Lastly, in some instances, we tested samples rather than the entire audit population. In those cases, the results cannot be projected to the population as that may be misleading.

Management Comments

MILLENNIUM
CHALLENGE CORPORATION
UNITED STATES OF AMERICA

DATE: October 21, 2019

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

FROM: James C. Porter /s/
Chief Information Officer
Department of Administration and Finance
Millennium Challenge Corporation

SUBJECT: MCC's Response to the Draft Audit Report, *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (A-MCC-20-00X-C), dated October 11, 2019

The Millennium Challenge Corporation (MCC) appreciates the opportunity to review the draft report on the Office of Inspector General (OIG)'s audit *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA*, dated October 11, 2019. MCC concurs with the conclusion of the report and deemed the report constructive in helping to validate the agency's compliance with the Federal Information Security Modernization Act of 2014 (FISMA).

Our Management Response to your recommendations are as follows:

Recommendation 1. Create a monitoring plan to review and update policy, procedures, and agreements in accordance with the timeliness requirements established in agency policies.

MCC Management Response: MCC concurs with this recommendation. MCC's Chief Information Officer (CIO) will create a monitoring plan to review and update policies, procedures, and agreements in accordance with the timelines established in agency policies by April 30, 2020.

Recommendation 2. Revise the contingency plan to accurately identify the alternate processing site and associated procedures.

MCC Management Response: MCC concurs with this recommendation. MCC's CIO will revise its information technology contingency plan to accurately identify the alternate processing site and associated procedures by September 30, 2020.

Recommendation 3. In consultation with business owners, determine what information systems need to be prioritized for recovery; then, update the business process analysis and contingency plan to reflect these priorities.

MCC Management Response: MCC concurs with this recommendation. MCC's CIO will consult with MCC business owners to determine and prioritize information system recovery, and then update the contingency plan with the business process analysis by September 30, 2020.

Recommendation 4. Develop a procedure for contingency situations that defines the information technology personnel, their roles, responsibilities, and authorities and that defines when they will receive contingency training upon assuming those roles.

MCC Management Response: MCC concurs with this recommendation. With consultation of MCC's business owners, MCC's CIO will prioritize information system recovery and develop a procedure for contingency situations that defines the information technology personnel, roles, responsibilities, authorities; and training requirements by September 30, 2020.

If you have any questions or require any additional information, please contact James Porter at 202-521-3716 or porterjc@mcc.gov; or Jude Koval, Director of Internal Controls and Audit Compliance (ICAC), at 202-521-7280 or Kovaljg@mcc.gov.

CC: Alvin Brown, Deputy Assistant Inspector General for Audit, OIG, USAID
Lisa Banks, Assistant Director, Information Technology Audits Division, OIG, USAID
Ken Jackson, Vice President and Chief Financial Officer, A&F, MCC
Adam Bethon, Deputy Chief Financial Officer, A&F, MCC
Alice Miller, Chief Risk Officer, ARC, A&F, MCC
Chris Ice, Senior Director, OCIO, A&F, MCC
Miguel Adams, Chief Information Security Officer, OCIO, A&F, MCC
Jude Koval, Director, ICAC, ARC, A&F, MCC

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	2
AC-2	Account Management	2
AC-8	System Use Notification	3
AC-17	Remote Access	1
AR-4	Privacy Monitoring and Auditing	1
AR-5	Privacy Awareness and Training	1
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	3
CA-3	Systems Interconnections	2
CA-5	Plan of Action and Milestones	2
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	2
CM-6	Configuration Settings	1
CM-7	Least Functionality	3
CM-8	Information System Component Inventory	3
CM-10	Software Usage Restrictions	3
CP-1	Contingency Planning Policy and Procedures	2
CP-2	Contingency Plan	2
CP-3	Contingency Training	2
CP-4	Contingency Plan Testing	2
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
IR-1	Incident Response Policy and Procedures	1
IR-4	Incident Handling	1
IR-6	Incident Reporting	1
IR-7	Incident Response Assistance	1
MP-3	Media Marking	1

Control	Control Name	Number of Systems Tested
MP-6	Media Sanitization	1
PL-2	System Security Plan	4
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
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	4
SA-2	Allocation of Resources	2
SA-3	System Development Life Cycle	2
SA-4	Acquisition Process	2
SA-8	Security Engineering Principles	2
SA-9	External Information System Services	1
SC-7	Boundary Protection	1
SC-8	Transmission Confidentiality and Integrity	1
SC-18	Mobile Code	2
SC-28	Protection of Information at Rest	2
SE-2	Privacy Incident Response	1
SI-2	Flaw Remediation	2
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	1
SI-7	Software, Firmware, and Information Integrity	1