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

MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA

AUDIT REPORT A-MCC-21-001-C
NOVEMBER 5, 2020

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, and Inter-American Foundation.

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 5, 2020

TO: MCC, Vice President, Department of Administration and Finance, Ken Jackson

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

SUBJECT: MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA (A-MCC-21-001-C)

Enclosed is the final audit report on the Millennium Challenge Corporation's (MCC) information security program for fiscal year 2020 in support of 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 inventory dated January 2020. Fieldwork covered MCC's headquarters in Washington, DC, from April 22 to August 31, 2020, for the period from October 1, 2019, through August 31, 2020.

[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 115 of 120[2] 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 accurate inventory of hardware and software assets.

However, as summarized in the table below, RMA noted weaknesses in three of the eight FISMA metric domains.

Fiscal Year 2020 IG FISMA Metric Domains[3]	**Weaknesses Identified**
Risk Management	
Configuration Management	
Identity and Access Management	
Data Protection and Privacy	X
Security Training	X
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	X

To address the weaknesses identified in the report, we recommend that MCC's chief information officer take the following actions to address the Data Protection and Privacy and the Security Training domains.

Recommendation 1. Update the *Information System Security Policy* and *Privacy Policy* to align with agency practices.

Recommendation 2. Develop and administer role-based privacy training for personnel responsible for handling personally identifiable information.

[2] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the FY 2020 IG metrics. RMA tested all 86 controls. A control was counted for each system it was tested against. Thus, there were 120 instances of testing a control.

[3] Office of Management and Budget, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency's "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics" (April 17, 2020).

In addition, we made three recommendations in our 2019 FISMA audit report[4] to address the weaknesses in the Contingency Planning domain. However, MCC had not taken final corrective action on them during the audit. See Appendix II on page 13 of RMA's report for the full text of those three recommendations.

In finalizing the report, the audit firm evaluated MCC's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1 and 2 resolved but open pending completion of planned activities. Please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance provided to our staff and the audit firm's employees during the engagement.

[4] Recommendations 2, 3, and 4, "MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA" (A-MCC-20-001-C), November 12, 2019.

RMA Associates

Auditors. Consultants. Advisors.

Millennium Challenge Corporation (MCC)

Federal Information Security Modernization Act of 2014 (FISMA)

Final Report

FY 2020

RMA | Associates
Auditors. Consultants. Advisors.

October 22, 2020

Mr. Mark Norman
Director, Information Technology Audits Division
United States Agency for International Development
Office of 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, CFE, CGFM, CICA, CGMA, CDFM, CDPSE
President
RMA Associates, LLC

RMA | Associates
Auditors. Consultants. Advisors.

Inspector General
United States Agency for International Development
Washington, D.C.

October 22, 2020

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 covered MCC's headquarters located in Washington, D.C., from April 22, 2020, to August 31, 2020.

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. However, 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 three Inspector General (IG) FISMA Metric Domains mostly due to policy and procedures not being updated with the organization's current practices. We made two recommendations to assist MCC in strengthening its information security program. In addition, three findings related to recommendations from the prior year are still open.

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

Respectfully,

RMA Associates

RMA Associates, LLC
Arlington, VA

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) 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 sources. 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 (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 OMB and congressional committees on the effectiveness of their information security program.

FISMA also requires agency IGs to assess the effectiveness of agency information security programs and practices to determine the effectiveness of such program and practices, and to report the results of the assessments to the Office of Management and Budget (OMB).

Annually, OMB and the Department of Homeland Security (DHS) provide instructions to Federal agencies and IGs for assessing agency information security programs. On November 19, 2019, OMB issued OMB Memorandum M-20-04, "Fiscal Year 2019-2020 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.

The FY 2020 metrics are designed to assess the maturity[4] of an information security

[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.

[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.

program and align with the five functional areas in the NIST Cybersecurity Framework, Version 4.0: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2020 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2020 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

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require 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 115 of 120[5] instances of security controls. For example, MCC:

- Maintained security plans that explicitly define the authorization boundary for their systems.
- Maintained a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Maintained an effective procedure to continuously monitor the network for unauthorized software.
- Maintained an accurate inventory of hardware and software assets.

[5] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the FY 2020 IG metrics. We tested all 86 controls. A control was counted for each system it was tested against. Thus, there were 120 instances of testing a control. See Appendix III for a list of the controls.

Although MCC generally implemented an effective information security program, its implementation of 5 of 120 instances of selected controls was not fully effective in preserving the confidentiality, integrity, and availability of the agency's information and information systems. As a result, we noted weaknesses in the following 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 Weaknesses Noted in FY 2020 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2020 IG FISMA Metric Domains	Weakness Noted in FY 2020
Identify	Risk Management	No Weakness Identified.
Protect	Configuration Management	No Weakness Identified.
	Identity and Access Management	No Weakness Identified.
	Data Protection and Privacy	MCC Needs to Align Information Security and Privacy Training Policy with Practices (Finding 1).
	Security Training	MCC Needs to Administer Role-Based Privacy Training to Personnel Having Responsibility for Personally Identifiable Information (PII) (Finding 2).
Detect	Information Security Continuous Monitoring	No Weakness Identified.
Respond	Incident Response	No Weakness Identified.
Recover	Contingency Planning	MCC Needs to Identify the Alternate Processing Site (Finding 3). MCC Needs to Identify Priority Information Systems Required for Business Processes (Finding 4). MCC Needs to Define Procedures for Identifying Individuals Assuming IT Contingency Roles and for Completing Contingency Training (Finding 5).

In addition, as illustrated in Appendix II, Status of Prior Year Findings, three of four prior year recommendations had not yet been fully implemented, and therefore, new recommendations were not made to address those weaknesses. Detailed findings appear in the following section.

Audit Findings

1. MCC Needs to Align Information Security and Privacy Training Policy with Practices.

Cybersecurity Framework Security Function: *Protect*
FY20 FISMA Metrics Area: *Security Training*

MCC grants users access to information systems before the completion of Information Security and Privacy Training. Also, MCC's current practice is that new hires have ten days to complete security awareness training. However, this practice is contrary to MCC's policies stated below.

The MCC *Privacy Policy AF-2010-7.4* dated January 19, 2016 states "Users must receive privacy awareness training prior to being granted access to the MCC network and systems."

The MCC *Information System Security Policy A&F-2009-46.4* dated October 30, 2015, states "All personnel, contractors, or others working on behalf of MCC accessing MCC systems shall receive initial training and annual refresher training. Users shall complete training within twenty-four (24) hours of being granted a user account."

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4 Security Awareness and Training Policy and Procedures AT-1 states:

> The organization:
>
> b. Reviews and updates the current:
>
> 1. Security awareness and training policy [Assignment: organization-defined frequency]; and
>
> 2. Security awareness and training procedures [Assignment: organization-defined frequency].

MCC stated that users are granted access to information systems before the completion of Information Security and Privacy Training as they would require access to the system in order to complete the training because the courses are on MCC's network.

Furthermore, due to an oversight, MCC did not update its *Information System Security Policy A&F-2009-46.4* to properly reflect the current practices MCC has regarding the timely completion of security awareness training for their new employees and contractors.

Without completing security training, MCC employees and contractors may not be aware of the potential security risk and perform actions that may affect the confidentiality, integrity, and availability of information for MCC.

Recommendation 1: We recommend MCC's Chief Information Officer update its *Information System Security Policy A&F-2009-46.4* and *Privacy Policy AF-2010-7.4* to align with agency practices.

2. MCC Needs to Administer Role-Based Privacy Training to Personnel Having Responsibility for Personally Identifiable Information (PII).

Cybersecurity Framework Security Function: *Protect*
FY20 FISMA Metrics Area: *Data Protection and Privacy*

MCC did not administer role-based privacy training for its two personnel that have significant responsibility for handling personally identifiable information (PII) as stated in their *Privacy Policy AF-2010-7.4.*

MCC's Privacy Policy dated January 19, 2016 states:

> The CPO [chief privacy officer] must:
>
> 2. Provide targeted, role-based training to employees who are designated Custodians who have greater responsibilities for privacy information and handle or process PII in the routine performance of their jobs.

NIST SP 800-53, Revision 4 Privacy Awareness and Training AR-5 states:

> The organization:
>
> b. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and
>
> c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].

The MCC Chief Information Security Officer was not aware of NIST SP 800-53, Rev 4, the requirement to administer role-based privacy training to personnel having the responsibility of PII in accordance with the AR-5 privacy control.

Without proper role-based privacy training, MCC could be at risk of improperly handling activities that involve PII.

Recommendation 2: We recommend that MCC's Chief Information Officer develop and administer role-based privacy training for personnel having responsibility for handling personally identifiable information.

3. MCC Needs to Identify the Alternate Processing Site.

Cybersecurity Framework Security Function: *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.

NIST SP 800-53, Revision 4 Alternate Processing Site CP-7 states:

> 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.

A recommendation addressing this finding was issued in the fiscal year 2019 FISMA audit report.[6] Because that recommendation is still open, we are not making a new recommendation at this time.

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

Cybersecurity Framework Security Function: *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

[6] Recommendation 2 in *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (Audit Report No. A-MCC-20-001-C, November 12, 2019).

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.

NIST SP 800-53, Revision 4 Contingency Planning CP-2 states:

> 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.

A recommendation addressing this finding was issued in the fiscal year 2019 FISMA audit report.[7] Because that recommendation is still open, we are not making a new recommendation at this time.

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

Cybersecurity Framework Security Function: *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.

[7] Recommendation 3 in *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (Audit Report No. A-MCC-20-001-C, November 12, 2019).

NIST SP 800-53, Revision 4 Contingency Plan Testing CP-3 states:

> 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.

A recommendation addressing this finding was issued in the fiscal year 2019 FISMA audit.[8] Because that recommendation is still open, we are not making a new recommendation at this time.

[8] Recommendation 4 in *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (Audit Report No. A-MCC-20-001-C, November 12, 2019).

Evaluation of Management Comments

In response to the draft report, MCC outlined its plans to address the two recommendations. MCC's comments are included in their entirety in Appendix IV.

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

Appendix I – Scope and Methodology

Scope

RMA conducted this audit in accordance with GAGAS, as specified in GAO'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 security controls for selected information systems[9] in support of FISMA.

The audit included tests 86 of management, technical, and operational controls outlined in NIST SP 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 controls related to the FY 2020 IG FISMA Reporting Metrics from four of seven judgmentally selected information systems in MCC's FISMA inventory as of January 2020. See Appendix III for a listing of the 120 control instances that we tested.[10]

The audit also included a follow up on four prior audit recommendations[11] to determine if MCC made progress in implementing the recommended improvements concerning its information security program. See Appendix II for the status of prior year recommendations.

Audit fieldwork covered MCC's headquarters located in Washington, D.C., from April 22, 2020, to August 31, 2020. It covered the period from October 1, 2019, through August 31, 2020.

[9] See Appendix III for a list of controls and the number of systems tested.
[10] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the FY 2020 IG metrics. We tested all 86 controls. A control was counted for each system it was tested against. Thus, there were 120 instances of testing a control. See Appendix III for a list of the controls.
[11] *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (Audit Report No. A-MCC-20-001-C, November 12, 2019).

Methodology

To perform our audit of MCC's information security program and practices, we followed a work plan based on the OMB and DHS, FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics. We reviewed legal and regulatory requirements stipulated in FISMA and conducted interviews with MCC officials and contractors to determine if MCC implemented an effective information security program. 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. Furthermore, we reviewed the status of FISMA audit recommendations for FY 2019.

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 the 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.

Appendix II – Status of Prior Year Findings

The following table provides the status of the FY 2019 FISMA audit recommendations.[12]

Table 3: FY 2019 FISMA Audit Recommendations

		Should the recommendation be closed?	
No.	**FY 2019 Audit Recommendations**	**MCC Position**	**Auditor's Position**
1	Create a monitoring plan to review and update policy, procedures, and agreements in accordance with the timeliness requirements established in agency policies.	Yes	Agree
2	Revise the contingency plan to accurately identify the alternate processing site and associated procedures.	No	Agree, see finding 3
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.	No	Agree, see finding 4
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.	No	Agree, see finding 5

[12] *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (Audit Report No. A-MCC-20-001-C, November 12, 2019).

Appendix III – Summary of Controls Reviewed

The following table identifies the controls selected for testing.

Table 4: Summary of Controls Reviewed

No. of Controls in IG Metrics	Control	Control Name	Number of Systems Tested
1	AC-1	Access Control Policy and Procedures	1
2	AC-2	Account Management	4
3	AC-5	Separation of Duties	4
4	AC-6	Least Privilege	4
5	AC-8	System Use Notification	1
6	AC-11	Session Lock	1
7	AC-12	Session Termination	1
8	AC-17	Remote Access	1
9	AC-19	Access Control for Mobile Devices	1
10	AU-2	Audit Events	1
11	AU-3	Content of Audit Records	1
12	AU-6	Audit Review, Analysis, And Reporting	1
13	AT-1	Security Awareness and Training Policy and Procedures	1
14	AT-2	Security Awareness Training	1
15	AT-3	Role-Based Security Training	1
16	AT-4	Security Training Records	1
17	CM-1	Configuration Management Policy and Procedures	1
18	CM-2	Baseline Configuration	1
19	CM-3	Configuration Change Control	1
20	CM-4	Security Impact Analysis	1
21	CM-6	Configuration Settings	1
22	CM-7	Least Functionality	1
23	CM-8	Information System Component Inventory	1
24	CM-9	Configuration Management Plan	1
25	CM-10	Software Usage Restrictions	1
26	CP-1	Contingency Planning Policy and Procedures	1
27	CP-2	Contingency Plan	1
28	CP-3	Contingency Training	1
29	CP-4	Contingency Plan Testing and Exercises	1
30	CP-6	Alternate Storage Site	1
31	CP-7	Alternate Processing Site	1
32	CP-8	Telecommunications Services	1
33	CP-9	Information System Backup	1
34	IA-1	Identification and Authentication Policy and Procedures	1
35	IA-2	Identification and Authentication (Organizational Users)	1
36	IA-4	Identifier Management	1

No. of Controls in IG Metrics	Control	Control Name	Number of Systems Tested
37	IA-5	Authenticator Management	1
38	IA-7	Cryptographic Module Authentication	1
39	IA-8	Identification and Authentication (Non-Organizational Users)	1
40	IR-1	Incident Response Policy and Procedures	1
41	IR-4	Incident Handling	1
42	IR-6	Incident Reporting	1
43	IR-7	Incident Response Assistance	1
44	MP-3	Media Marking	1
45	MP-6	Media Sanitization	1
46	PS-1	Personnel Security Policy and Procedures	1
47	PS-2	Position Risk Designation	1
48	PS-3	Personnel Screening	1
49	PS-6	Access Agreements	1
50	PL-2	System Security Plan	4
51	PL-4	Rules of Behavior	1
52	PL-8	Information Security Architecture	1
53	PM-5	Information System Inventory	1
54	PM-7	Enterprise Architecture	1
55	PM-8	Critical Infrastructure Plan	1
56	PM-9	Risk Management Strategy	1
57	PM-11	Mission/Business Process Definition	1
58	RA-1	Risk Assessment Policy and Procedures	1
59	RA-2	Security Categorization	4
60	RA-5	Vulnerability Scanning	1
61	CA-1	Security Assessment and Authorization Policies and Procedures	4
62	CA-2	Security Assessments	4
63	CA-3	System Interconnections	2
64	CA-5	Plan of Action & Milestones (POA&Ms)	3
65	CA-6	Security Authorization	3
66	CA-7	Continuous Monitoring	3
67	SC-7(10)	Boundary Protection| Prevent Unauthorized Exfiltration	1
68	SC-8	Transmission Integrity	1
69	SC-10	Network Disconnect	1
70	SC-13	Cryptographic Protection	1
71	SC-18	Mobile Code	1
72	SC-28	Protection of Information at Rest	1
73	SI-2	Flaw Remediation	1
74	SI-3	Malicious Code Protection	1
75	SI-4	Information System Monitoring	4
76	SI-4(4)	Information System Monitoring| Inbound and Outbound	1

No. of Controls in IG Metrics	Control	Control Name	Number of Systems Tested
		Communications Traffic	
77	SI-4(18)	Information System Monitoring| Analyze Traffic/Cover Exfiltration	1
78	SI-7(8)	Software, Firmware, and Information Integrity| Auditing Capability for Significant Events	1
79	SA-3	System Development Life Cycle	1
80	SA-4	Acquisition Process	1
81	SA-8	Security Engineering Principles	1
82	SA-9	External Information System Services	4
83	SA-12	Supply Chain Protection	1
84	SE-2	Privacy Incident Response	1
85	AR-4	Privacy Monitoring and Auditing	1
86	AR-5	Privacy Awareness and Training	1
TOTAL CONTROL INSTANCES TESTED			**120**

Appendix IV – Management Comments

DATE: October 14, 2020

TO: Alvin Brown
Deputy Assistant Inspector General for Audit
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 2020 in Support of FISMA* (A-MCC-21-XXX-C), dated September 22, 2020

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 2020 in Support of FISMA*, dated September 22, 2020. 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).

In regards to the three FY 2019 FISMA audit recommendations, MCC provided final action and requested closure for each recommendation on September 15, 2020. As of the date of our response, the OIG has not officially closed these recommendations. Our Management Response to your FY 2020 recommendations are as follows:

Recommendation 1. Update the *Information System Security Policy* and *Privacy Policy* to align with agency practices.

MCC Management Response: MCC concurs with this recommendation. MCC CIO will update and align the *Information System Security Policy* and *Privacy Policy* to agency practices by February 5, 2021.

Recommendation 2. Develop and administer role-based privacy training for personnel responsible for handling personally identifiable information.

MCC Management Response: MCC concurs with this recommendation. MCC CIO will develop and administer role-based privacy training for personnel responsible for handling personally identifiable information by March 31, 2021.

If you have any questions or require any additional information, please contact me 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: Mark Norman, Director, Information Technology Audits Division, 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
Lori Giblin, 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