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

MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA

Audit Report A-MCC-23-002-C
September 5, 2023

Information Technology Audits Division

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

MEMORANDUM

DATE: September 5, 2023

TO: MCC, Chief Information Officer and Chief Privacy Officer, Christopher E. Ice

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

SUBJECT: MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA (A-MCC-23-002-C)

Enclosed is the final audit report on the Millennium Challenge Corporation's (MCC) information security program for fiscal year 2023, in support of the Federal Information Security Modernization Act of 2014 (FISMA).[1] 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.[2] To answer the audit objective, RMA assessed the effectiveness of MCC's implementation of the FY 2023 IG FISMA reporting metrics[3] that fall into the nine domains in

[1] Pursuant to the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, § 5274, which amends the Inspector General Act of 1978, when USAID OIG contracts with an audit firm to perform the work, USAID OIG provides non-governmental organizations and/or business entities specifically identified in the accompanying report, if any, 30 days from the date of report publication to review the final report and submit a written response to USAID OIG that clarifies or provides additional context for each instance within the report in which the non-governmental organization and/or business entity is specifically identified. Any comments received to this effect are posted for public viewing on https://usaid.oig.gov with USAID OIG's final transmittal. Please direct related inquiries to oignotice_ndaa5274@usaid.gov.

[2] For this audit, an effective information security program was defined as having an overall mature program based on the current year inspector general FISMA reporting metrics.

[3] Office of Management and Budget and Council of the Inspectors General on Integrity and Efficiency's "FY 2023 - 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," February 10, 2023.

the following table. Also, RMA assessed MCC's implementation of selected management, technical, and operational controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations," updated December 2020.

RMA reviewed 4 of the 13 judgmentally selected systems in MCC's inventory as of October 19, 2022. Fieldwork covered MCC's headquarters in Washington, DC, from September 15, 2022, to June 22, 2023, for the period from October 1, 2022, through June 22, 2023.

RMA concluded that MCC generally implemented an effective information security program, considering the unique mission, resources, and challenges of the agency. For example, MCC:

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Maintained an accurate inventory of hardware and software assets.
- Employed automated mechanisms to test system contingency plans.

However, as summarized in the table below, RMA found weakness in all nine IG FISMA metric domains.

Fiscal Year 2023 IG FISMA Metric Domains	**Weaknesses Identified**
Risk Management	X
Supply Chain 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

To address the weaknesses identified in the report, we recommend that MCC's Chief Information Officer take the following actions:

Recommendation 1. Update the agency's policies and procedures to reflect security controls identified in National Institute of Standards and Technology Special Publication 800-53, Revision 5.

Recommendation 2. Develop and implement a plan for Millennium Challenge Corporation's security assessments to be updated.

Recommendation 3. Implement level 2 event logging requirements in accordance with Office of Management and Budget memorandum M-21-31.

Recommendation 4. Develop and implement a process to make periodic updates to the Millenium Challenge Corporation's business impact assessments.

In finalizing the report, RMA evaluated MCC's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1, 2, 3 and 4 resolved but open pending completion of planned activities. For recommendations 1 through 4, please provide evidence of final action to OIGAuditTracking@usaid.gov.

In addition, of six open recommendations from the FY2021 FISMA audit, MCC took final action to close four recommendations, action to close one recommendation will be assessed at a later time, and one recommendation remains open.[4] Refer to Appendix II on page 13 of RMA's report for the status of prior year recommendations.

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

[4] Recommendations 3, 4, 5, and 6 were closed, action to close recommendation 7 will be assessed later, and recommendation 2 remains open in *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report No. A-MCC-22-004-C, December 2, 2021).

RMA | Associates

Auditors. Consultants. Advisors.

Millenium Challenge Corporation (MCC)

Federal Information Security Modernization Act of 2014 (FISMA)

Final Report
Fiscal Year 2023

RMA | Associates
Auditors. Consultants. Advisors.

September 5, 2023

Ms. Lisa Banks
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 Ms. Banks:

RMA Associates, LLC, is pleased to present our report on Millennium Challenge Corporation's (MCC) compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023.

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.

September 5, 2023

RMA Associates, LLC, 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 scope of this audit was to assess MCC's information security program consistent with FISMA and reporting instructions issued by the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency. The audit included tests of management, technical, and operational controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, updated September 2020.

For this audit, we reviewed 4 of 13 judgmentally selected systems in MCC's inventory as of October 19, 2022. Audit fieldwork covered MCC's headquarters located in Washington, D.C., from September 15, 2022, to June 22, 2023.

Our audit was performed in accordance with *Generally Accepted Government Auditing Standards*, as specified in 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.

We found weaknesses in MCC's security posture in preserving the agency's information and information systems' confidentiality, integrity, and availability. Consequently, we noted weaknesses in all nine Inspector General FISMA Metric Domains primarily due to MCC not updating its policies and procedure in accordance with National Institute of Standards and Technology Special Publication 800 Revision 5. We made four recommendations to assist MCC in strengthening its information security program. Nonetheless, we concluded that MCC implemented an effective information security program, considering the unique mission, resources, and challenges of the agency.

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 evaluation of the Millennium Challenge Corporation's (MCC) information security program for fiscal year (FY) 2023. The objective of this performance audit was to determine whether MCC implemented an effective information security program.[2]

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.

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.

FISMA also requires the agency Inspectors General (IGs) to assess the effectiveness of agency information security programs and practices and report the results of the assessments to the Office of Management (OMB).

The FY 2023 metrics are designed to assess the maturity[3] of an information security program and align with the five functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1.

[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 having an overall mature program based on the current year Inspector General FISMA reporting metrics.

[3] 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.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2023 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain 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

This 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 objective. RMA believes the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Audit Results

The audit concluded that MCC generally implemented an effective information security program, considering the unique mission, resources, and challenges of the agency. For example, MCC:

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Maintained an accurate inventory of hardware and software assets.
- Employed automated mechanisms to test system contingency plans.

As shown in Table 2, the overall maturity level of MCC's information security program was Managed and Measurable (Effective).

Table 2: FY 2023 MCC Maturity Level

Cybersecurity Framework Security Functions	FY 23 Assessed Maturity Level	Effective?
Identify	Consistently Implemented	No
Protect	Managed and Measurable	Yes
Detect	Managed and Measurable	Yes
Respond	Managed and Measurable	Yes
Recover	Managed and Measurable	Yes
Overall	**Managed and Measurable**	Yes

However, weaknesses were identified in MCC's security posture in preserving the confidentiality, integrity, and availability of its information and information systems. All nine IG FISMA metric domains had weaknesses related to policies and procedures not being updated to reflect NIST Special Publication (SP) 800-53, Revision 5. In addition, four domains had other weaknesses (Table 3).

Table 3: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2023 FISMA Assessment

Cybersecurity Framework Security Functions	**FY 2023 IG FISMA Metric Domains**	**Weakness Noted in FY 2023**
Identify	Risk Management	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1)
	Supply Chain Risk Management	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1) MCC Needs to Fully Develop its Supply Chain Risk Management Strategy, Policies, and Procedures (Finding 2)
Protect	Configuration Management	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1)
	Identity and Access Management	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1)
	Data Protection and Privacy	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1)
	Security Training	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1)
Detect	Information Security Continuous Monitoring	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1) MCC Did Not Always Update its Security Assessments. (Finding 3)
Respond	Incident Response	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1) MCC Did Not Fully Comply with the Event Logging Requirements (Finding 4)

Cybersecurity Framework Security Functions	FY 2023 IG FISMA Metric Domains	Weakness Noted in FY 2023
Recover	Contingency Planning	MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5 (Finding 1) MCC Needs to Update its Business Impact Analysis (Finding 5)

We are making four new recommendations to address the identified weaknesses. In addition, as illustrated in Appendix II, we assessed the status of five of six prior FISMA audit recommendations and determined that MCC took final corrective action on four but not one of them. We will evaluate the remaining recommendation later. Detailed findings appear in the following section.

Audit Findings

1. MCC Needs to Update its Policies and Procedures to Incorporate Updates in NIST SP 800-53 Revision 5.

Cybersecurity Framework Security Function: *All Functions*
FY23 IG FISMA Metric Domain: *All Domains*

MCC did not update the following policy and procedures to incorporate updates in NIST SP Revision 5:

- Access Control Procedure
- Information System Security Policy
- Privacy Policy
- Contingency Planning Procedure
- MCC Physical Access Controls: Franklin Court OCIO – 2018-PR-PSO1
- Physical & Environmental Protection Procedures: Franklin Court Data Closets
- Privacy Procedure
- System and Services Acquisition Procedure

NIST SP 800-53, Revision 5, has 20 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].

According to MCC officials, due to competing priorities, MCC did not update its policies and procedures, as required. MCC was updating the security plan for one of its systems and merging two system security packages to streamline their security assessment and authorization process. Further, MCC had to address the additional controls typically covered by the cloud service provider.

As a result, MCC's policies and procedures did not fully cover important security controls to preserve the confidentiality, integrity, and availability of the agency's information and information systems.

Recommendation 1: *We recommend that MCC's Chief Information Officer update the agency's policies and procedures to reflect security controls identified in National Institute of Standards and Technology Special Publication 800-53, Revision 5.*

2. MCC Needs to Fully Develop its Supply Chain Risk Management Strategy, Policies, and Procedures.

Cybersecurity Framework Security Function: *Identify*
FY21 IG FISMA Metric Domain: *Supply Chain Risk Management*

MCC's supply chain risk management (SCRM) strategy, policies, and procedures did not define the minimum requirements. Specifically, MCC's SCRM AF-2020-2.0 Section 889 Purchasing Policy and FY 22 Purchase Card Standard Operating Procedures did not define:

- SCRM risk appetite and tolerance.
- SCRM strategies or controls.
- Processes for consistently evaluating and monitoring supply chain risk.
- Approaches for implementing and communicating the SCRM strategy.
- Procedures to facilitate the implementation of the policy and the associated baseline supply chain risk management controls as well as baseline supply chain-related controls in other families.

Public law 115-390 – 115th Congress, Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the "SECURE Technology Act" (December 31, 2018) requires executive agencies to develop an overall SCRM strategy and implementation plan and policies and processes to guide and govern SCRM activities.

In addition, NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Chapter 2, section 2.2.1 FRAME, states:

> An organization Information and Communication Technology (ICT) SCRM policy is a critical vehicle for guiding ICT SCRM activities. Driven by applicable laws and regulations, this policy should support applicable organization policies including acquisition and procurement, information security, quality, and supply chain and logistics. It should address goals and objectives articulated in the overall agency strategic plan, as well as specific mission functions and business goals, along with the internal and external customer requirements. It should also define the integration points for ICT SCRM with the agency's Risk Management Process and System Development Life Cycle (SDLC).

Although MCC developed some policies and procedures for SCRM, according to MCC officials, the strategy, policies, and procedures were not complete because they were waiting for the Cybersecurity and Infrastructure Security Agency guidance for vendor attestations to be finalized. Further, MCC officials said that they need additional funding to complete the SCRM strategies, policies, and procedures.

Without established strategies, policies, and procedures, there is an increased risk that MCC's supply chain may become compromised, affecting the confidentiality, integrity, and availability of MCC's information and information systems. For example, MCC is at risk that it may not identify network devices manufactured by blacklisted companies or that it may purchase software compromised by hackers. A recommendation addressing this finding was made in the FY 2021 FISMA audit report.[4] Because that recommendation is still open, we are not making a new recommendation at this time.

[4] Recommendation 1 in *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report A-MCC-22-004-C, December 2, 2021).

3. MCC Did Not Always Update its Security Assessments

Cybersecurity Framework Security Function: *Detect*
FY23 IG FISMA Metric Domain: *Information Security Continuous Assessment*

For one of the four systems reviewed, MCC did not update its security assessments, as required. Specifically, that security assessment was last updated May 2021, thus exceeding by one year MCC's requirement to make updates every 12-18 months.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* states:

> **CA-7 CONTINUOUS MONITORING**
>
> Control: Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organizational level continuous monitoring strategy that includes:
>
> c. Ongoing control assessments in accordance with the continuous monitoring strategy

In addition, MCC's Security Authorization and Assessment Procedure (March 2022) states:

> 3.3 Frequency of the Security Authorization Process
>
> - MCC will actively review and update at least 33 percent of the NIST 800-53 rev 4 security controls of every accredited system every 12-18 months so that an Authority to Operate (ATO) can be granted every three-year interval.

According to MCC officials, the system inherited controls from the general support and cloud systems that MCC was in the process of merging, which caused the delay of conducting the security assessment. In addition, MCC did not have a plan for updating its security assessments.

Without an up-to-date security assessment, MCC may have unidentified vulnerabilities, weaknesses, or gaps in its control measures. As a result, MCC may be susceptible to cybersecurity threats, data breaches, and non-compliance with regulations.

Recommendation 2: *We recommend that MCC's Chief Information Officer develop and implement a plan for its security assessments to be updated.*

4. MCC Did Not Fully Comply with the Event Logging Requirements.

Cybersecurity Framework Security Function: *Respond*
FY23 IG FISMA Metric Domain: *Incident Response*

MCC did not meet the Event Logging Level 2 (EL2), intermediate, requirements as specified in OMB M-21-31. Although MCC captured the necessary information from the logs and stored the log data offline, MCC did not fulfill the requirement to maintain 12 months of log information accessible online. Further, MCC did not implement EL2, intermediate log requirements. For example, MCC did not log the date, time, source, and destination of cyber incidents.

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, states that, to meet EL2, agencies must meet the following requirements:

> - EL1 maturity level
> - Intermediate Logging Categories [See Appendix III of this report for details]
> - Publication of Standardized Log Structure
> - Inspection of Encrypted Data
> - Intermediate Centralized Access
>
> …
>
> Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:
> […]
> Within one year of the date of this memorandum, reach EL1 maturity.
> Within 18 months of the date of this memorandum, achieve EL2 maturity.
> Within two years of the date of this memorandum, achieve EL3 maturity.
>
> …
>
> The Retention Period required the utilization of the 12 Months Active Storage and 18 Months Cold Data Storage.

MCC did not meet the logging requirements at the maturity EL2 (intermediate) level due to the complexity and volume of logging requirements, including logging types, log retention, and log management. According to MCC officials, MCC met the logging types outlined in OMB M-21-31 for EL2 after May 2023. In addition, MCC did not have adequate storage capacity to retain the last 12 months of active logs. According to MCC officials, MCC now has the capacity to retain the last 12 months of active data with the installation of its new intrusion detection system.

By not fully meeting the EL2 (intermediate) logging requirements, MCC may not be able to accelerate incident response efforts to enable more effective defense of the agency's information.

Recommendation 3: *We recommend that MCC's Chief Information Officer implement level 2 event logging requirements in accordance with Office of Management and Budget M-21-31.*

5. MCC Needs to Update its Business Impact Analysis.

Cybersecurity Framework Security Function: *Recover*
FY23 IG FISMA Metric Domain: *Contingency Planning*

MCC did not review and update its Enterprise Business Impact Analysis (BIA) at least every two years, as required. The BIA was last reviewed and updated in August 2020—over two and a half years ago.

Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process,* Annex D: Business Impact Analysis states:

> D-1: A formal review, update, and validation of the organization's essential functions through a BIA must be conducted at least every two years. As part of biennial continuity assessments conducted by FEMA, D/As must affirm that risks to the performance of its MEFs and PMEFs have been evaluated and documented as part of its BIA.

NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems*,* states:

> Chapter 3: Information System Contingency Planning Process
> This section describes the process to develop and maintain an effective information system contingency plan. The process presented is common to all information systems. The seven steps in the process are:
>
> 1. Develop the contingency planning policy;
> 2. Conduct the business impact analysis (BIA);
> 3. Identify preventive controls;
> 4. Create contingency strategies;
> 5. Develop an information system contingency plan;
> 6. Ensure plan testing, training, and exercises; and
> 7. Ensure plan maintenance.

According to MCC officials, MCC's BIA surpassed the two-year update requirement due to an ongoing management review. The purpose of that review was to align MCC's business impact with its information technology enterprise resources in support of mission essential functions. In addition, MCC did not update the BIA because there was a delay in MCC's coordination with the Federal Emergency Management Agency's National Continuity Program on the updates. Further, MCC did not develop and implement a process to make periodic updates for its business impact assessments. Nonetheless, inaccurate BIAs increase the risk that the agency will be unable to prioritize recovery operations effectively in the event of a service interruption.

Recommendation 4: *We recommend that MCC's Chief Information Officer develop and implement a process to make periodic updates of its business impact assessments.*

Evaluation of Management Comments

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

Based on our evaluation of management comments, we acknowledge MCC's management decisions on all four recommendations. Further, we consider recommendations 1, 2, 3 and 4 resolved, but open pending completion of planned activities.

Appendix I – Scope and Methodology

Scope

RMA Associates, LLC (RMA) conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability's Office *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. Our audit was conducted for fiscal year (FY) 2023 and tested the core and supplemental metrics identified in the *FY 2023 - 2024 Inspector General (IG) Federal Information Modernization Act of 2014 (FISMA) Reporting Metrics* issued by OMB and the Council of the Inspectors General on Integrity and Efficiency.

The scope of this audit was to assess MCC's information security program consistent with FISMA and reporting instructions issued by the Office of Management and Budget and the DHS. In addition, the audit included tests of management, technical, and operational controls outlined in National institute Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.* We assessed MCC's performance and compliance with FISMA in the following control areas:

- Risk Management
- Supply Chain 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 4 of 13 judgmentally selected systems in MCC's inventory as of October 19, 2022. The audit also included a follow-up on five prior audit recommendations[5] to determine if MCC had made progress in implementing the recommended improvements concerning its information security program. See Appendix II for status or prior year recommendations.

Audit fieldwork was conducted at MCC's headquarters located in Washington, DC, from September 15, 2022, to June 22, 2023. It covered the period from October 1, 2022, through June 22, 2023.

Methodology

To determine if MCC implemented an effective information security program, RMA conducted interviews with MCC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. Additionally, RMA reviewed documentation supporting the information security program. These documents included, but were not

[5] Recommendations 2-6 in *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report A-MCC-22-004-C, December 2, 2021).

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. RMA compared documentation against requirements stipulated in NIST SP's. Also, RMA performed tests of information system controls, including a vulnerability assessment, to determine the effectiveness of those controls. Furthermore, RMA reviewed the status of FISMA audit recommendations for FY 2021.

In testing the effectiveness of the security controls, RMA exercised professional judgment in determining the number of items selected for testing and the method used to select them. RMA considered the relative risk and the significance of the specific items in achieving the related control objectives. In addition, RMA 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, RMA tested judgmental 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 Recommendations

The following table provides the status of the FY 2021 FISMA audit recommendations.[6][7]

Table 4: FY 2021 FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2021 Audit Recommendations	MCC's Position	Auditor's Position on the Status
A-MCC-22-004-C (Rec.2)	Develop and document supply chain policies, procedures, and strategies.	Open	Agree Refer to Finding #2
A-MCC-22-004-C (Rec.3)	Revise and implement MCC's Vulnerability Patch Compliance Policy to align with timeframes in the Department of Homeland Security's Fiscal Year 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.	Closed	Agree
A-MCC-22-004-C (Rec.4)	Develop and implement a process to conduct an independent periodic review of MCC's privacy program.	Closed	Agree
A-MCC-22-004-C (Rec.5)	Fully develop and implement a security awareness training strategy.	Closed	Agree
A-MCC-22-004-C (Rec.6)	Document and implement a process to monitor and enforce MCC's procedures for security training.	Closed	Agree
A-MCC-22-004-C (Rec.7)	Document and implement a written process for obtaining and evaluating feedback on MCC's privacy and security training content, including role-based training.	Closed	Will be assessed later

[6] RMA only evaluated recommendations that pertain to the core and current year supplemental metrics. The remaining recommendation will be evaluated later.

[7] *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report A-MCC-22-004-C, December 2, 2021).

Appendix III – OMB M-21-31 Event Log Level 2 Requirements

According to OMB-M-21-31, agencies must implement the following Event Log Level 2 requirements:

- Network Device Infrastructure (for Devices with Multiple Interfaces: Interface Media Access Control (MAC) - If Correlated to the De-NAT Internet Protocol (IP) Address) - All Devices: IDs / IPs Alerts and Events
    - Date and Time
    - Source
        - Hostname
        - IP Address and Port
        - MAC
    - Destination
        - Hostname
        - IP Address and Port
        - MAC
    - Signature Triggered and Associated Details Including:
        - Signature
        - Anomaly
    - Rate Threshold
    - Device Name
    - Type of Event and Category
    - In the Case of Fortinet Network IPs, Attack Context
    - (Web / Device) User Agent if Available
    - Wi-Fi Channel
    - Wi-Fi Extended Service Set Identifier (ESSID)
- Application Level - Web Applications
    - Uniform Resource Locator (URL)
    - Headers
    - Hypertext Transfer Protocol (HTTP) Methods - Request with Body of Data14
    - HTTP Response with Body of Data
- Network Traffic - Full Packet Capture Data
    - Decrypted Plaintext
    - Cleartext
- Application Level - General – Non- Commercial Off the Shelf (COTS)
    - User Authentication (Success/Failure)
    - User Access of Application Components
        - File and Object Access
        - Audit Log Access (Success/Failure)
        - System Access (Failure)
        - Application Transactions
    - Transaction Logs
    - System Performance and Operational Characteristics
        - Resource Utilization

    - Errors (Input Validation, Dis-allowed Operations)
    - Process Status
    - Service Status Changes (e.g., Started, Stopped)
  - Application Configuration and Version, Middleware Configuration and Version
  - Usage Information, if Applicable
  - User Request and Response Events, if Applicable

Appendix IV – Management Comments

MILLENNIUM
CHALLENGE CORPORATION
UNITED STATES OF AMERICA

DATE: August 17, 2023

TO: Alvin Brown
Deputy Assistant Inspector General for Audit
Office of Inspector General
United States Agency for International Development
Millennium Challenge Corporation

FROM: Christopher Ice Miguel Adams /s/ Acting CIO for
Chief Information Officer
Department of Administration and Finance
Millennium Challenge Corporation

SUBJECT: MCC's Management Response to the Draft Audit Report, *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA*, dated August 3, 2023

The Millennium Challenge Corporation (MCC) appreciates the opportunity to review the draft report on the Office of Inspector General's (OIG) audit, *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA*, dated August 3, 2023. MCC concurs with the conclusions 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). MCC continues to work towards developing and documenting supply chain policies, procedures, and strategies as identified in Recommendation 2 in the FY 2021 FISMA Audit Report. MCC expects to complete this final action during FY 2024. MCC's Management Response to each recommendation is below.

Recommendation 1 *– Update the agency's policies and procedures to reflect security controls identified in National Institute of Standards and Technology Special Publication 800-53, Revision 5.*

MCC Management Response: MCC concurs with this recommendation. MCC will update the agency's policies and procedures to reflect security controls identified in National Institute of Standards and Technology Special Publication 800-53, Revision 5 no later than September 15, 2024.

Recommendation 2 *– Develop and implement a plan for Millenium Challenge Corporation's security assessments to be updated.*

MCC Management Response: MCC concurs with this recommendation. MCC will develop and implement a plan to update security assessments by March 15, 2024.

Recommendation 3 *– Implement level 2 event logging requirements in accordance with Office of Management and Budget Memorandum M-21-31.*

MCC Management Response: MCC concurs with this recommendation. MCC will implement level 2 event logging requirements in accordance with Office of Management and Budget memorandum M-21-31 by September 15, 2024.

Recommendation 4 *– Develop and implement a process to make periodic updates to the Millenium Challenge Corporation's business impact assessments.*

MCC Management Response: MCC concurs with this recommendation. MCC will develop and implement a process to make periodic updates to MCC's business impact assessments by January 12, 2024.

If you have any questions or require any additional information, please contact me at 202-521-2652 or icece@mcc.gov; or Jude Koval, Senior Director of Internal Controls and Audit Compliance (ICAC), at 202-521-7280 or Kovaljg@mcc.gov.

CC: Lisa Banks, Director, Information Technology Audits Division, OIG, USAID
Fouad Saad, 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
Miguel Adams, Chief Information Security Officer, OCIO, A&F, MCC
Jude Koval, Senior Director, ICAC, ARC, A&F, MCC