FISMA: Despite Challenges, MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2024

Audit Report A-MCC-24-001-C

August 22, 2024

MEMORANDUM

DATE: August 22, 2024

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

FROM: Paul K. Martin, Inspector General /s/

SUBJECT: FISMA: Despite Challenges, MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2024 (A-MCC-24-001-C)

Enclosed is the final audit report on the Millennium Challenge Corporation's (MCC) information security program for fiscal year (FY) 2024, 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 2024 IG FISMA reporting metrics[3] that fall into the nine domains in the following table. Also, RMA assessed MCC's implementation of applicable controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 5,

---

[1] Pursuant to the Pub. L. No. 117-263 § 5274, USAID OIG provides nongovernmental organizations and/or businesses specifically identified in this report 30 days from the date of report publication to submit a written response to USAID OIG. Any comments received will be posted on https://oig.usaid.gov/. Please direct inquiries to oignotice_ndaa5274@usaid.gov

[2] For this audit, an effective information security program is defined as having an overall mature program based on the current year IG 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.

"Security and Privacy Controls for Federal Information Systems and Organizations," updated December 2020.

RMA reviewed 4 judgmentally selected systems of the 13 in MCC's inventory as of October 16, 2023. RMA's work covered MCC's headquarters in Washington, DC, from September 15, 2023, to May 29, 2024, for the period from October 1, 2023, through May 29, 2024.

RMA concluded that MCC generally implemented an effective information security program. 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.

• Centrally managed its flaw remediation process and used automated patch management and software update tools for operating systems where such tools were available and safe.

• Implemented an enterprise-wide single sign-on solution.

• Provided its personnel with awareness and specialized training that produced a demonstrable improvement in phishing exercises.

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

Fiscal Year 2024 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

RMA also determined that MCC did not take final action on four prior recommendations from the FY 2021 and FY 2023 FISMA audits.[4] MCC officials explained that they were having challenges implementing the recommendations due to competing priorities within their information security program and a lack of timely Federal guidance for new control requirements. Refer to Appendix II of RMA's report for the status of prior year recommendations.

We are making one new recommendation in addition to the four prior FISMA audit recommendations that MCC has not yet implemented. To address the new weakness identified in the report, we recommend that MCC's Chief Information Officer take the following action:

Recommendation 1. Implement level 3 event logging requirements in accordance with Office of Management and Budget Memorandum M-21-31.

In finalizing the report, RMA evaluated MCC's response to the recommendation. After reviewing that evaluation, we consider recommendation 1 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] Recommendation 2 in *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (A-MCC-22-004-C), December 2, 2021, and recommendations 1, 2, and 3 in *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (A-MCC-23-002-C), September 5, 2023.

RMA | Associates
Auditors. Consultants. Advisors.

Millennium Challenge Corporation (MCC)
Federal Information Security Modernization Act of 2014
(FISMA)

Final Report
Fiscal Year 2024

RMA | Associates
Auditors. Consultants. Advisors.

August 22, 2024

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:

The independent certified public accounting firm, 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 2024.

Thank you for the opportunity to serve your organization and the assistance provided by your staff and 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

Inspector General
United States Agency for International Development
Washington, D.C.   August 22, 2024

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 whether MCC's information security program was consistent with FISMA, and reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security. The audit included tests of applicable 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.
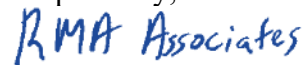
For this audit, we reviewed 4 judgmentally selected systems of 13 in MCC's inventory as of October 16, 2023. Audit covered MCC's headquarters located in Washington, D.C., from September 15, 2023, to May 29, 2024.

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

We concluded that MCC implemented an effective information security program. However, 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 procedures in accordance with the National Institute of Standards and Technology Special Publication 800 Revision 5. To assist MCC in strengthening its information security program, we made one new recommendation in addition to the four prior FISMA audit recommendations that MCC has not yet implemented.

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 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) 2024. 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).

Annually, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) provide instructions to Federal agencies and IGs for assessing agency information security programs. The FY 2024 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.

Audit Results

The audit concluded that MCC generally implemented an effective information security program. For example, MCC:

- Maintained an effective process for assessing the risk associated with positions involving information system duties.

---

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the 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 was 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.

- Maintained an accurate inventory of hardware and software assets.
- Centrally managed its flaw remediation process and used automated patch management and software update tools for operating systems where such tools were available and safe.
- Implemented an enterprise-wide single sign-on solution. All systems interfaced with the solution, resulting in an ability to centrally manage privileged user accounts.
- Provided its personnel with awareness and specialized training that produced a demonstrable improvement in phishing exercises.

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

Table 1: FY 2024 MCC Maturity Level

Cybersecurity Framework Security Functions	Core Metrics	FY 24 Supplemental Metrics	FY 24 Assessed Maturity Level
Identify	Effective	Not Effective	Consistently Implemented
Protect	Effective	Effective	Managed and Measurable
Detect	Not Effective	Effective	Consistently Implemented
Respond	Not Effective	Effective	Consistently Implemented
Recover	Effective	Effective	Managed and Measurable
Overall	Not Effective	Effective	**Managed and Measurable**

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, three domains had other weaknesses (Table 3).

Table 2: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2024 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains	Weakness Noted in FY 2024
Identify	Risk Management	MCC Needs to Update its Policies and Procedures to Incorporate NIST SP 800-53 Revision 5 (Finding 1)

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains	Weakness Noted in FY 2024
	Supply Chain Risk Management	MCC Needs to Update its Policies and Procedures to Incorporate 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 NIST SP 800-53 Revision 5 (Finding 1)
	Identity and Access Management	MCC Needs to Update its Policies and Procedures to Incorporate NIST SP 800-53 Revision 5 (Finding 1)
	Data Protection and Privacy	MCC Needs to Update its Policies and Procedures to Incorporate NIST SP 800-53 Revision 5 (Finding 1)
	Security Training	MCC Needs to Update its Policies and Procedures to Incorporate NIST SP 800-53 Revision 5 (Finding 1)
Detect	Information Security Continuous Monitoring	MCC Needs to Update its Policies and Procedures to Incorporate NIST SP 800-53 Revision 5 (Finding 1) MCC Needs to Perform its Security Assessments Annually (Finding 3)
Respond	Incident Response	MCC Needs to Update its Policies and Procedures to Incorporate NIST SP 800-53 Revision 5 (Finding 1) MCC Needs to Implement Event Logging Requirements (Finding 4)
Recover	Contingency Planning	MCC Needs to Update its Policies and Procedures to Incorporate NIST SP 800-53 Revision 5 (Finding 1)

We are making one new recommendation in addition to the four prior FISMA audit recommendations that MCC has not yet implemented. (See the "Audit Findings" section.) Appendix II illustrates that MCC took final corrective actions on two of six prior FISMA audit recommendations that were open at the beginning of audit fieldwork. MCC officials explained that competing priorities within their information security program and a lack of timely federal guidance toward new control requirements were the main challenges faced by the agency toward addressing the remaining four recommendations.

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*

As previously reported,[4] MCC did not update the following policies and procedures to incorporate updates in NIST SP 800-53, 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*
- *Supply Chain Risk Management Policy and 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, the transition to NIST SP 800-53, Revision 5, is still underway due to competing priorities. MCC performs procedural updates every two years, and updates were not completed at the time of this audit. For instance, according to MCC officials, the Access Control policy and procedure document was updated to address the NIST SP 800-53, Revision 5 controls; however, it was still under review and had not been signed. As a result, MCC's policies and procedures did not address the additional control families and enhancements in NIST SP 800-53, Revision 5, necessary to preserve the confidentiality, integrity, and availability of the agency's information and information systems. A recommendation addressing this finding was made in the FY 2023 FISMA audit report.[5] Because that recommendation is still open, we are not making a new recommendation at this time.

---

[4] *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report No. A-MCC-23-002-C, September 5, 2023).
[5] Recommendation 1 in *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report No. A-MCC-23-002-C, September 5, 2023).

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*

As previously reported,[6] 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
- Detection of counterfeit components
- 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 Supply Chain Risk Management (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's 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).

Further, NIST SP 800-161, control SR-11 titled Component Authenticity, states:

> The development of anti-counterfeit policies and procedures requires input from and coordination with acquisition, information technology, IT security, legal, and the C-SCRM PMO. The policy and procedures should address regulatory

---

[6] *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).

compliance requirements, contract requirements or clauses, and counterfeit reporting processes to enterprises, such as GIDEP and/or other appropriate enterprises. Where applicable and appropriate, the policy should also address the development and use of a qualified bidders list (QBL) and/or qualified manufacturers list (QML). This helps prevent counterfeits through the use of authorized suppliers, wherever possible, and their integration into the organization's supply chain [CISA SCRM WG3].

According to MCC officials, the strategy, policies, and procedures were incomplete because they were awaiting guidance from the Cybersecurity and Infrastructure Security Agency, which was not issued until March 2024. MCC made progress by creating an internal attestation tracker for all critical software and submitting completed attestation forms to the Cybersecurity and Infrastructure Security Agency's Repository for Software Attestations and Artifacts. The repository allows federal agencies with the same vendors to leverage completed attestation forms toward their IT environments.

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 it may purchase software compromised by hackers. A recommendation addressing this finding was made in the FY 2021 FISMA audit report.[7] Because that recommendation is still open, we are not making a new recommendation at this time.

3. MCC Needs to Perform its Security Assessments Annually
Cybersecurity Framework Security Function: *Detect*
FY23 IG FISMA Metric Domain: *Information Security Continuous Assessment*

As previously reported,[8] MCC did not perform its security assessment as required for one of the four systems reviewed. Specifically, that security assessment was last performed in May 2021, which exceeded the threshold by more than two years, thus exceeding the 12–18-month due date for making updates. In FY 22, no security controls assessment was performed. According to MCC officials, in FY 23, the decision was made to merge the security packages from the general support system and a cloud system. MCC planned to perform the security controls assessment on July 15, 2023. However, due to competing priorities, the security controls assessment was not completed until November 17, 2023—an additional four-month delay.

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

---

[7] Recommendation 2 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).
[8] *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report No. A-MCC-23-002-C, September 5, 2023).

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.

MCC may have unidentified vulnerabilities, weaknesses, or gaps in its control measures that would go undetected without an up-to-date security assessment. As a result, MCC may be susceptible to cybersecurity threats, data breaches, and non-compliance with regulations. A recommendation addressing this finding was made in the FY 2023 FISMA audit report.[9] Because that recommendation is still open, we are not making a new recommendation at this time.

4. MCC Needs to Implement Event Logging Requirements
Cybersecurity Framework Security Function: *Respond*
FY23 IG FISMA Metric Domain: *Incident Response*

MCC did not meet the event logging (EL) requirements at maturity EL2 (intermediate) level, in accordance with OMB M-21-31. MCC was required to reach EL2 maturity within 18 months of the memorandum, which was issued on August 27, 2021. As of May 25, 2024, or 33 months since issuance, MCC was at maturity EL1 (basic) level. Furthermore, the memorandum set forth the deadline of August 2023 for adherence to EL3 (advanced) requirements, which MCC did not meet.

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021) states:

Section I: Maturity Model for Event Log Management
Tier EL2, Rating – Intermediate
The agency and all of its components meet the following requirements, as detailed in Table 3 (EL2 Intermediate Requirements) within Appendix A (Implementation and Centralized Access Requirements):
- Meeting EL1 maturity level

---

[9] Recommendation 2 in *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report No. A-MCC-23-002-C, September 5, 2023).

- Intermediate Logging Categories
- Publication of Standardized Log Structure
- Inspection of Encrypted Data
- Intermediate Centralized Access

Section II: Agency Implementation Requirements

Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:
[…]
Within 18 months of the date of this memorandum, achieve EL2 maturity.
Within two years of the date of this memorandum, achieve EL3 maturity.

Appendix B: EL2 Intermediate Requirements – Inspection of Encrypted Data

Federal agencies shall retain and store in clear text form the data or Encrypted Data metadata from Appendix C that is collected in their environment. If agencies perform full traffic inspection through active proxies, they should log additional available fields as described in Appendix C and can work with CISA to implement these capabilities. If agencies do not perform full traffic inspection, they should log the metadata available to them. In general, agencies are expected to follow zero-trust principles concerning least privilege and reduced attack surface, and relevant guidance from OMB and CISA relating to zero-trust architecture.

According to MCC officials, system limitations prevented MCC from logging metadata, so MCC could not perform full traffic inspections to meet the Inspection of Encrypted Data requirement set forth by OMB M-21-31. By not meeting the Inspection of Encrypted Data requirement for maturity EL2 (intermediate), MCC does not follow the zero-trust principle concerning least privilege or reduce the attack surface that can be exploited in a cyberattack scenario. A recommendation addressing EL2 was made in the FY 2023 FISMA audit report.[10] Because that recommendation is still open, we are not making a new recommendation at this time. Nonetheless, we are making the following recommendation to help MCC meet EL3 logging requirements.

Recommendation 1: *We recommend that the Millenium Challenge Corporation's Chief Information Officer implement level 3 event logging requirements in accordance with Office of Management and Budget memorandum M-21-31.*

---

[10] Recommendation 3 in *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (Audit Report No. A-MCC-23-002-C, September 5, 2023).

Evaluation of Management Comments

In response to the draft report, MCC outlined its plan to address recommendation 1. MCC's comments are included in their entirety in Appendix III. Based on our evaluation of management comments, we acknowledge management decision on recommendation 1. Further, the recommendation is resolved, but open pending completion of planned activities.

Appendix I – Scope and Methodology

Scope
RMA conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office *Government Auditing Standards*. These 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our audit was conducted for FY 2024 and tested the core and supplemental metrics identified in the *FY 2023 - 2024 IG FISMA Reporting Metrics* issued by OMB and CIGIE.

The scope of this audit was to assess MCC's information security program, which is consistent with FISMA and reporting instructions issued by OMB and the CIGIE. In addition, the audit included tests of applicable controls outlined in NIST 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

We conducted a risk assessment to identify a representative number of systems (a minimum of two internal and two external) to be tested when needed for system-level testing. Only moderate systems not tested in the prior year or not part of continuous monitoring were selected for FY 2024. Four out of thirteen internal and external systems were selected for FY 2024 in MCC's current system inventory as of October 2, 2023, to meet the requirement. For this audit, we reviewed the four judgmentally selected systems out of thirteen in MCC's inventory as of October 16, 2023.

The audit also included a follow-up on six prior audit recommendations[11,12] to determine if MCC had made progress in implementing the recommended improvements concerning its information security program. See Appendix II for the status of recommendations for the prior year.

---

[11] Recommendations 2 and 7 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).
[13] Recommendations 1-4 in *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).
.

The audit was conducted at MCC's headquarters located in Washington, DC, from September 15, 2023, to May 29, 2024. It covered the period from October 1, 2023, through May 29, 2024.

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 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 special publications. 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 and FY 2023.

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, 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, 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.[13]

Table 3: FY 2021 FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2021 Audit Recommendations	MCC's Corrective Action	MCC's Position	Auditor's Position
A-MCC-22-004-C (Rec. 2)	We recommend that the Millenium Challenge Corporation's Chief Information Officer develop and document supply chain policies, procedures, and strategies.		Open	Agree
A-MCC-22-004-C (Rec. 7)	We recommend that the Millenium Challenge Corporation's Chief Information Officer document and implement a written process for obtaining and evaluating feedback on MCC's privacy and security training content, including role-based training.	Documented and implemented a written process for obtaining and evaluating feedback on MCC's privacy and security training content, including role-based training.	Closed	Agree

The following table provides the status of the FY 2023 FISMA audit recommendations.[14]

Table 5: FY 2023 FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2023 Audit Recommendations	MCC's Corrective Action	MCC's Position	Auditor's Position
A-MCC-23-002-C (Rec. 1)	We recommend that the Millenium Challenge Corporation's Chief Information Officer update the agency's policies and procedures to reflect security controls identified in NIST SP 800-53, Revision 5.		Open	Agree
A-MCC-23-002-C (Rec. 2)	We recommend that the Millennium Challenge Corporation's Chief Information Officer develop and implement a plan for Millennium Challenge Corporation's security assessments to be updated.		Open	Agree

---

[13] *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).

[14] *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).

Audit Report & Recommendation No.	FY 2023 Audit Recommendations	MCC's Corrective Action	MCC's Position	Auditor's Position
A-MCC-23-002-C (Rec. 3)	We recommend that the Millenium Challenge Corporation's Chief Information Officer implement EL2 logging requirements in accordance with OMB M-21-31.		Open	Agree
A-MCC-23-002-C (Rec. 4)	We recommend that MCC's Chief Information Officer develop and implement a process to make periodic updates to the Millennium Challenge Corporation's business impact assessments.	Developed and formalized the Millennium Challenge Corporation 2023-2025 Business Process Analysis and Business Impact Analysis. This document describes the process related to the business impact analysis.	Closed	Agree

Appendix III – Management Comments

DATE: July 23, 2024

TO: Gabriele A. Tonsil
            Deputy Assistant Inspector General for Audit
            Office of Inspector General
            United States Agency for International Development
            Millennium Challenge Corporation

FROM: Christopher Ice
            Chief Information Officer
            Department of Administration and Finance
            Millennium Challenge Corporation

SUBJECT: MCC's Management Response to the Draft Audit Report, *FISMA: Despite Challenges, MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2024*, dated July 17, 2024

The Millennium Challenge Corporation (MCC) appreciates the opportunity to review the draft report on the Office of Inspector General's (OIG) audit, *FISMA: Despite Challenges, MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2024*, dated July 17, 2024.   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. Additionally, MCC submitted a final action in June 2024 related to FY 2023 FISMA Report Recommendation 2. MCC expects to submit final actions for the remaining FY 2023 FISMA Report Recommendations by the end of this fiscal year. MCC's Management Response to the new FY 2024 recommendation is below.

Recommendation 1 – *Implement level 3 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 3 event logging requirements in accordance with Office of Management and Budget memorandum M-21-31 by September 19, 2025.

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