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

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

Information Technology Audits Division

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

MEMORANDUM

DATE: December 2, 2021

TO: MCC, Acting Vice President and Chief Financial Officer, Brian Corry

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

SUBJECT: MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA (A-MCC-22-004-C)

Enclosed is the final audit report on the Millennium Challenge Corporation's (MCC) information security program for fiscal year 2021, 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 evaluated the effectiveness of MCC's implementation of the FY 2021 Inspector General (IG) FISMA reporting metrics[2] that fall into the nine domains in the following table. Also, RMA assessed 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 reviewed four of the seven information systems in MCC's inventory dated

[1] 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.

[2] Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics," May 12, 2021.

February 8, 2021. Audit fieldwork covered MCC's headquarters located in Washington, DC, from March 22, 2021, to September 9, 2021. It covered the period from October 1, 2020, through September 9, 2021.

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

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Conducted an annual contingency plan exercise and captured lessons learned and test results, as appropriate.
- Maintained an effective process for tracking and reporting verified incidents.

However, as summarized in the table below, RMA noted weaknesses in six of the nine FY 2021 IG FISMA metrics domains.

Fiscal Year 2021 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	
Incident Response	
Contingency Planning	

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

Recommendation 1. Develop and implement processes to document and implement lessons learned related to risk management, configuration management, and identity and access management.

Recommendation 2. Develop and document supply chain policies, procedures, and strategies.

Recommendation 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.

Recommendation 4. Develop and implement a process to conduct an independent periodic review of MCC's privacy program.

Recommendation 5. Fully develop and implement a security awareness training strategy.

Recommendation 6. Document and implement a process to monitor and enforce MCC's procedures for security training.

Recommendation 7. Document and implement a written process for obtaining and evaluating feedback on MCC's privacy and security training content, including role-based training.

In finalizing the report, the audit firm evaluated MCC's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1 through 7 resolved but open pending completion of planned activities. For the seven recommendations, 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.

RMA | Associates

Auditors. Consultants. Advisors.

Millennium Challenge Corporation (MCC)

Federal Information Security Modernization Act of 2014 (FISMA)

Final Report
Fiscal Year 2021

RMA | Associates
Auditors. Consultants. Advisors.

November 30, 2021

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 the Millennium Challenge Corporation's (MCC) compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2021.

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. November 30, 2021

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 reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security. The audit included tests of management, technical, and operational 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*, updated January 22, 2015.

For this audit, we reviewed four of seven judgmentally selected systems in MCC's inventory as of February 8, 2021. Audit fieldwork covered MCC's headquarters located in Washington, D.C., from March 22, 2021, to September 9, 2021.

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 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 six out of nine Inspector General FISMA Metric Domains mostly due to lessons learned not being conducted and documented and not collecting feedback on the content of its security and privacy training. We made seven recommendations to assist MCC in strengthening its information security program.

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 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) 2021. 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 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 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 9, 2020, OMB issued OMB Memorandum M-21-02, "*Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements.*" According to that memorandum, each year, IGs are required to complete metrics[3] to independently assess their agencies' information security programs.

The FY 2021 metrics are designed to assess the maturity[4] of an information security program and align with the five functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 4.0: 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 was defined as having an overall mature program based on the current year Inspector General FISMA reporting metrics.

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

[4] The five maturity levels are: 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 2021 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2021 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 implemented an effective information security program. For example, MCC:

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

- Conducted an annual contingency plan exercise, captured lessons learned and test results, as appropriate; and

- Maintained an effective process for tracking and reporting verified incidents.

The overall maturity level of MCC's information security program was Managed and Measurable.[5] We have presented the maturity level for the nine domains below:

Table 2: MCC’s FY 2021 Maturity Levels

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metric Domains	Maturity Level
Identify	Risk Management	Consistently Implemented
Identify	Supply Chain Risk Management[6]	Ad Hoc
Protect	Configuration Management	Defined
Protect	Identity and Access Management	Consistently Implemented

[5] A program at that assessed level is considered effective by OMB and DHS.

[6] To provide agencies with sufficient time to implement NIST SP 800-53, Revision 5, the Supply Chain Risk Management domain was not used to calculate the Identify framework function rating or the overall maturity level.

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metric Domains	Maturity Level
Protect	Data Protection and Privacy	Managed and Measurable
Protect	Security Training	Defined
Detect	Information Security Continuous Monitoring	Consistently Implemented
Respond	Incident Response	Managed and Measurable
Recover	Contingency Planning	Managed and Measurable
Overall		**Managed and Measurable**

However, we found weaknesses in MCC's security posture in preserving the confidentiality, integrity, and availability of the agency's information and information systems. As a result, we noted weaknesses in six out of nine IG FISMA Metric Domains (Table 3) and presented recommendations to assist the agency in strengthening its information security program. We noted that three of the domains had weaknesses related to lessons learned not being conducted and documented and two of the domains had weaknesses related to the collection of feedback on the content of its security and privacy training.

Table 3: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2021 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metric Domains	Weakness Noted in FY 2021
Identify	Risk Management	MCC Needs to Fully Conduct and Document Lessons Learned (Finding 1).
Identify	Supply Chain Risk Management	MCC Needs to Develop and Document Supply Chain Risk Management Policies, Procedures, and Strategies (Finding 2).
Protect	Configuration Management	MCC Needs to Fully Conduct and Document Lessons Learned (Finding 1). MCC Needs to Remediate Vulnerabilities Within MCC's Defined Remediation Timeframe and Revise Its Policies and Procedures Based on the DHS FISMA Guidance (Finding 3).
Protect	Identity and Access Management	MCC Needs to Fully Conduct and Document Lessons Learned (Finding 1).
Protect	Data Protection and Privacy	MCC Needs to Perform an Independent Review of Its Privacy Program (Finding 4). MCC Needs to Collect

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metric Domains	Weakness Noted in FY 2021
		Feedback on the Content of Its Security and Privacy Training (Finding 7).
Protect	Security Training	MCC Needs to Fully Develop a Security Awareness and Training Strategy (Finding 5). MCC Needs to Ensure Annual Security Awareness Training for Users Is Completed in the Defined Time Period. (Finding 6). MCC Needs to Collect Feedback on the Content of Its Security and Privacy Training (Finding 7).
Detect	Information Security Continuous Monitoring	No Weakness Identified.
Respond	Incident Response	No Weakness Identified.
Recover	Contingency Planning	No Weakness Identified.

We are making seven recommendations to address the weaknesses identified. In addition, as illustrated in Appendix II, two prior year recommendations were fully implemented. Detailed findings appear in the following section.

Audit Findings

1. MCC Needs to Fully Conduct and Document Lessons Learned.

Cybersecurity Framework Security Function: *Identify and Protect*
FY21 IG FISMA Metric Domain: *Risk Management, Configuration Management, and Identity and Access Management*

MCC did not document lessons learned for the following FISMA Functions and Domains:

- Identify (Risk Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)

NIST *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.1 states:

> Functions organize basic cybersecurity activities at their highest level. These functions are Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.
>
> Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

In addition, NIST Special Publication (SP) 800-37 Revision 2 *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy*, states:

> …to incorporate lessons learned as continuous monitoring and ongoing authorization processes are implemented for moderate impact and high-impact systems. Incorporating lessons learned facilitates the consistent progression of the continuous monitoring and ongoing authorization implementation from the lowest to the highest impact levels for the systems.

This problem occurred because MCC management did not develop and implement a process to document and implement lessons learned to improve its security posture.

Without a formal, disciplined lesson learned process, MCC may not capture information from its practices to identify areas of improvement. Therefore, MCC may lose the opportunity to strengthen its security posture against actual risk events.

Recommendation 1: *We recommend that MCC's Chief Information Officer develop and implement processes to document and implement lessons learned related to risk management, configuration management, and identity and access management.*

2. MCC Needs to Develop and Document Supply Chain Risk Management Policies, Procedures, and Strategies.

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

MCC did not develop and document policies, procedures, and strategies to evaluate its supply chain risk appetite and tolerance and to continuously monitor and evaluate supply chain risks.

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 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).

According to MCC officials, MCC purchases all supply chain related components directly from approved governments vendors. As such, they did not believe additional controls were required as the impact of risk was low. In addition, MCC officials stated that Supply Chain Risk Management is a new domain in FY2021 IG FISMA Reporting Metrics and, because the required controls were outlined in NIST SP 800-53 Revision, Revision 5, they had until September 2021 to implement them.

Without established policies, procedures, and strategies, there is an increased risk that MCC's supply chain may become compromised, affecting MCC’s data confidentiality, integrity, and availability. 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.

Recommendation 2: *We recommend that MCC's Chief Information Officer develop and document supply chain policies, procedures, and strategies.*

3. MCC Needs to Remediate Vulnerabilities Within MCC's Defined Remediation Timeframe and Revise Its Policies and Procedures Based on the DHS FISMA Guidance.

Cybersecurity Framework Security Function: *Protect*
FY21 IG FISMA Metric Domain: *Configuration Management*

MCC did not remediate its vulnerabilities within MCC's defined timeframe. We identified 84 critical vulnerabilities and 398 high vulnerabilities that were not remediated in accordance with the timeframes in MCC's Vulnerability Patch Compliance policy. Approximately 87 percent of those critical and high vulnerabilities were over 60 days old. In addition, MCC did not have a process in place to patch critical vulnerabilities within 30 days, as stated in the FY 21 IG FISMA Reporting Metrics to meet the consistently implemented maturity level.

MCC's Vulnerability Patch Compliance Policy (August 2018) states:

> Critical/High-Need to be remediated within 45 days of first being identified by Nessus Security Center, IA, or issued by the Department of Homeland Securities National Cybersecurity and Communication Integration Center (NCCIC). All critical vulnerabilities identified by NCCIC must be remediated within 45 days of issuing the weekly Cyber Hygiene Report. If unable to mitigate a vulnerability within 45 days, a detailed justification needs to be submitted to the MCC CISO outlining any barriers, planned steps for resolution, and a timeframe for mitigation. The MCC CISO must report vulnerabilities not mitigated to NCCIC within 45 days from when NCCIC first identified the vulnerability.

In addition, NIST SP 800-53, Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations* states:

> **Sl-2 FLAW REMEDIATION**
>
> Control: The organization:
> a. identifies, reports, and corrects information system flaws;
> b. tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
> c. installs security-relevant software and firmware updates within [*Assignment: organization-defined period*] of the release of the updates; and
> d. incorporates flaw remediation into the organizational configuration management process.

Also, according to the FY 21 IG FISMA Reporting Metrics (May 12, 2021), Question 21, Consistently Implemented:

> The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a

> timely manner. In addition, the organization patches critical vulnerabilities within 30 days and utilizes lessons learned in implementation to make improvements to its flaw remediation policies and procedures.

MCC's process was to remediate critical vulnerabilities within 45 days. However, according to MCC officials, their process did not allow sufficient time to remediate vulnerabilities properly and they require more time to analyze and implement software patches.

Without remediating vulnerabilities in a timely manner, MCC could expose its network to cyberattacks and leave data susceptible to unauthorized disclosure and modification. Additionally, uncorrected vulnerabilities may lead to inappropriate or unnecessary changes to mission-focused information systems, resulting in compromising mission information or other sensitive data.

Recommendation 3: *We recommend that MCC's Chief Information Officer 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.*

4. MCC Needs to Perform an Independent Review of Its Privacy Program.

Cybersecurity Framework Security Function: *Protect*
FY21 IG FISMA Metric Domain: Data Protection and Privacy

MCC did not perform an independent review of its privacy program.

According to the FY 21 IG FISMA Reporting Metrics (May 12, 2021), Question 35, Managed and Measurable:

> The organization conducts an independent review of its privacy program and makes necessary improvements.

In addition, NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* states:

> **AR-4 PRIVACY MONITORING AND AUDITING**
>
> Control: The organization monitors and audits privacy controls and internal privacy policy [*Assignment: organization-defined frequency*] to ensure effective implementation.
>
> Supplemental Guidance: To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls

> by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems.

The independent review is a requirement in the FY 21 IG FISMA Reporting Metrics published in May 2021. MCC did not have an opportunity to implement a process to conduct periodic and independent reviews of its privacy program.

Without conducting an independent review of its privacy program, MCC may not have an objective evaluation of the structure and effectiveness of its privacy program and may not identify areas that need improvement.

Recommendation 4: *We recommend that MCC's Chief Information Officer develop and implement a process to conduct an independent periodic review of MCC's privacy program.*

5. MCC Needs to Fully Develop a Security Awareness and Training Strategy.

Cybersecurity Framework Security Function: *Protect*
FY21 IG FISMA Metric Domain: *Security Training*

MCC defined its security awareness and training strategy for developing, implementing, and maintaining security awareness and training program that is tailored to its mission and risk environment. However, MCC did not include all the components in its strategy. For example, the strategy did not include priorities, funding, the goals of the program, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools), and deployment methods.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003), states:

> **3.3 Developing an Awareness and Training Strategy and Plan**
>
> The plan should discuss the following elements:
>
> - Scope of the awareness and training program;
> - Roles and responsibilities of agency personnel who should design, develop, implement, and maintain the awareness and training material, and who should ensure that the appropriate users attend or view the applicable material;
> - Goals to be accomplished for each aspect of the program (e.g., awareness, training, education, professional development [certification]);
> - Topics to be addressed in each session or course;
> - Deployment methods to be used for each aspect of the program;

> **3.6 Funding the Security Awareness and Training Program**
>
> Once an awareness and training strategy has been agreed upon and priorities established, funding requirements must be added to the plan. A determination must be made regarding the extent of funding support to be allocated…

According to the MCC officials, they considered the strategy as part of their *Computer Security and Privacy Awareness Training Procedures*. However, the procedure did not address priorities, funding, the goals of the program, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools), and deployment methods. Also, MCC's funding for the current security awareness training is minimal. In addition, MCC plans to transition the responsibility for Security Awareness Training from its Chief Information Officer to its Human Resources office. As such, MCC Chief Information Officer did not develop a strategy.

Without a security awareness strategy, the agency cannot effectively integrate and focus its people, technology, and operations towards achieving MCC's security training goals.

Recommendation 5: *We recommend that MCC's Chief Information Officer fully develop and implement a security awareness training strategy.*

6. MCC Needs to Ensure Annual Security Awareness Training for Users Is Completed in the Defined Time Period.

Cybersecurity Framework Security Function: *Protect*
FY21 IG FISMA Metric Domain: *Security Training*

MCC's users did not always complete the annual security awareness training within 30 days as required by Agency policy. Forty-nine out of a population of 326 (15%) users did not complete the agency's FY 21 annual security awareness training by the due date.

NIST SP 800-53, Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations* states:

> **AT-2 SECURITY AWARENESS TRAINING**
>
> Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
> a. As part of initial training for new users;
> b. When required by information system changes; and
> c. [*Assignment: organization-defined frequency*] thereafter.

Due to the pandemic, MCC management deviated from their policy and did not enforce disabling users' accounts when the users did not complete the security awareness training. In addition, MCC did not have a process to monitor and enforce its procedures for security training.

Without the timely completion of security training, there is an increased risk of processing inaccurate, invalid, and unauthorized transactions, ultimately impacting system security. This could lead to the loss, destruction, and misuse of sensitive MCC data.

Recommendation 6: *We recommend that MCC's Chief Information Officer document and implement a process to monitor and enforce MCC's procedures for security training.*

7. MCC Needs to Collect Feedback on the Content of Its Security and Privacy Training.

Cybersecurity Framework Security Function: *Protect*
FY21 IG FISMA Metric Domain: *Data Protection and Privacy and Security Training*

MCC provides basic and role-based security and privacy training on an annual basis; however, they did not have a process to collect documented feedback on the content of these trainings from users.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003), states:

> **6.2 Evaluation and Feedback**
>
> Formal evaluation and feedback mechanisms are critical components of any security awareness, training, and education program. Continuous improvement cannot occur without a good sense of how the existing program is working. In addition, the feedback mechanism must be designed to address objectives initially established for the program.

MCC used commercial products for its training. According to MCC's officials, that training program did not change from year to year. As a result, MCC did not believe it was necessary to collect formal feedback from its users. As such, MCC did not have a process to obtain and evaluate feedback.

Without collecting feedback on the training content, MCC may not be able to gain insight on areas of improvement of the awareness and training program. Because security threats are constantly changing, security training should be revised to better prepare MCC in identifying and remediating emerging threats.

Recommendation 7: *We recommend that MCC'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.*

Evaluation of Management Comments

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

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

Appendix I - Scope and Methodology

Scope

RMA conducted this performance audit in accordance with generally accepted government auditing standards as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether MCC had 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 OMB and DHS. The audit included tests 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
- 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 four of seven judgmentally selected systems in MCC's inventory as of February 8, 2021. The audit also included a follow-up on two prior audit recommendations[7] to determine if MCC had 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 March 22, 2021, to September 9, 2021. It covered the period from October 1, 2020, through September 9, 2021.

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,

[7] Recommendations 1 and 2 in *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-MCC-21-001-C, November 5, 2020).

(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 to determine the effectiveness of those controls. Furthermore, RMA reviewed the status of FISMA audit recommendations from FY 2020.

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 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 2020 FISMA audit recommendations.[8]

Table 4: FY 2020 FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2020 Audit Recommendations	MCC's Position	Auditor's Position on the Status
A-MCC-21-001-C (Rec.1)	Update its *Information System Security Policy A&F-2009-46.4* and *Privacy Policy AF-2010-7.4* to align with agency practices.	Closed	Agree
A-MCC-21-001-C (Rec.2)	Develop and administer role-based privacy training for personnel having responsibility for handling personally identifiable information.	Closed	Agree

[8] *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-MCC-21-001-C, November 5, 2020).

Appendix III – Management Comments

MILLENNIUM
CHALLENGE CORPORATION
UNITED STATES OF AMERICA

DATE: October 14, 2021

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 /s/
Acting Chief Information Officer
Department of Administration and Finance
Millennium Challenge Corporation

SUBJECT: MCC's Management Response to the Draft Audit Report, *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA*, dated September 30, 2021

The Millennium Challenge Corporation (MCC) appreciates the opportunity to review the draft report on the Office of Inspector General's (OIG) audit, *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA*, dated September 30, 2021. 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's Management Response to each recommendation is below.

Recommendation 1 *– Develop and implement processes to document and implement lessons learned related to risk management, configuration management, and identity and access management.*

MCC Management Response: MCC concurs with this recommendation. MCC will develop and implement processes to document and implement lessons learned related to risk management, configuration management, and identity and access management no later than May 27, 2022.

Recommendation 2 *– Develop and document supply chain policies, procedures, and strategies.*

MCC Management Response: MCC concurs with this recommendation. MCC will document supply chain policies, procedures, and strategies by August 26, 2022.

Recommendation 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.*

MCC Management Response: MCC concurs with this recommendation. MCC will 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 by May 27, 2022.

Recommendation 4 *– Develop and implement a process to conduct an independent periodic review of MCC's privacy program.*

MCC Management Response: MCC concurs with this recommendation. MCC will develop and implement a process to conduct an independent periodic review of MCC's privacy program by Aug 31, 2022.

Recommendation 5 *– Fully develop and implement a security awareness training strategy.*

MCC Management Response: MCC concurs with this recommendation. MCC will fully develop and implement a security awareness training strategy by June 24, 2022.

Recommendation 6 *– Document and implement a process to monitor and enforce MCC's procedures for security training.*

MCC Management Response: MCC concurs with this recommendation. MCC will document and implement a process to monitor and enforce MCC's procedures for security training by April 27, 2022.

Recommendation *7 – Document and implement a written process for obtaining and evaluating feedback on MCC's privacy and security training content, including role-based training.*

MCC Management Response: MCC concurs with this recommendation. MCC will document and implement a written process for obtaining and evaluating feedback on MCC's privacy and security training content, including role-based training by March 25, 2022.

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: Mark Norman, Director, Information Technology Audits Division, OIG, USAID
Lisa Banks, Assistant Director, Information Technology Audits Division, OIG, USAID
Brian Corry, Acting 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