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

FISMA: MCC Implemented an Effective Information Security Program for FY 2025 Despite Some Concerns

Report A-MCC-26-002-M
January 15, 2026

Evaluation

Office of Audits, Inspections, and Evaluations

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

DATE: January 15, 2026

TO: Christopher E. Ice
Chief Information Officer and Chief Privacy Officer
Office of the Chief Information Officer
Millenium Challenge Corporation

FROM: Gabriele Tonsil /s/
Acting Assistant Inspector General for Audits, Inspections, and Evaluations

SUBJECT: FISMA: MCC Implemented an Effective Information Security Program for FY 2025 Despite Some Concerns

This memorandum transmits the final report on our evaluation of the Millennium Challenge Corporation's (MCC) information security program for fiscal year 2025, in support of the Federal Information Security Modernization Act of 2014 (FISMA). Our objective was to determine whether MCC implemented an effective information security program. In finalizing the report, we considered your comments on the draft and included them in their entirety in Appendix C.

The report contains two new recommendations to improve MCC's information security program. In addition, it identifies two recommendations from our prior FISMA audits that MCC has not yet implemented. After reviewing information you provided in response to the draft report, we consider recommendations 1 and 2 resolved but open pending completion of planned activities. For both recommendations, please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance you and your staff provided to us during this engagement.

Contents

Office of Inspector General
U.S. Agency for International Development

Report No A-MCC-26-002-M
January 15, 2026

Report in Brief

Why We Did This Evaluation

Implementing an effective information security program is crucial for protecting the confidentiality, integrity, and availability of Federal agencies' systems and the information they contain. Such safeguards address threats, ultimately protecting Americans and government resources from bad actors. To that end, the Federal Information Security Modernization Act of 2014 (FISMA) requires agency heads to implement policies and procedures to protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction. The statute also directs the USAID Office of Inspector General to annually assess the effectiveness of the Millennium Challenge Corporation's (MCC) information security program and practices and report the results of the assessments to the Office of Management and Budget (OMB).

In accordance with FISMA, we conducted this evaluation to determine whether MCC implemented an effective information security program. We focused on MCC's information security program for fiscal year (FY) 2025 through July 24, 2025, the date we reported the FISMA assessment results to OMB.

What We Recommend

We made two recommendations to improve MCC's security assessments of its internal and external information systems. In addition, we identified two recommendations from our prior FISMA audits that the Agency has not yet addressed.

What We Found

MCC implemented an effective information security program in FY 2025. For example, the Agency maintained a centralized, enterprise-wide view of cybersecurity risk management activities; an accurate inventory of hardware and software assets; phishing-resistant multifactor authentication mechanisms; required security controls; and specialized training for staff.

MCC did not fully implement supply chain procedures. The Agency issued supply chain procedures in response to a prior OIG recommendation but canceled or put on hold necessary procurement actions due to the administration's review of foreign assistance. A MCC official said the Agency expects to fully implement the procedures by December 2025. Doing so will better position MCC to mitigate the risk of threats from actors who can compromise the integrity of its information systems.

MCC did not ensure security assessments were performed for two significant systems. Agency officials said they intentionally delayed the security assessment for an internal system because they planned to make major changes to it and move it to a data center. MCC contracts with an external provider to host and operate an external system, but the contract did not require the provider to perform security assessments or state how often they should be performed. Thus, in addition to noncompliance with Federal requirements, MCC may be susceptible to cybersecurity threats and data breaches, putting sensitive Agency data at risk.

MCC did not implement two prior OIG FISMA recommendations. Specifically, the Agency did not implement a recommendation to update its policies and procedures to comply with National Institute of Standards and Technology requirements for security controls. MCC also did not implement certain event logging requirements established by OMB.

Introduction

Implementing an effective information security program is crucial for protecting the confidentiality, integrity, and availability of Federal agencies' systems and the information they contain. Such safeguards address threats, ultimately protecting Americans and government resources from bad actors. To that end, the Federal Information Security Modernization Act of 2014 (FISMA) requires OIG to annually assess the effectiveness of the Millennium Challenge Corporation's (MCC) information security program and practices and report the results of the assessments to the Office of Management and Budget (OMB).

We conducted this evaluation to determine whether MCC implemented an effective information security program.[1] Our review focused on MCC's information security program from October 1, 2024, through July 24, 2025, the date we reported our FISMA assessment results to OMB, with one exception: we reviewed the Agency's supporting documentation for one prior recommendation after that date.

To answer the objective, we followed OMB and the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) FY 2025 IG FISMA reporting metrics and FISMA Evaluator's Guide.[2] We ascertained the effectiveness of controls by reviewing MCC's policies and procedures related to information technology, vulnerability scans, security control assessment reports, privileged user security training material, and system inventories, among others. In addition, we interviewed Agency officials to gain an understanding of their information security practices and compliance with FISMA. For this evaluation, we judgmentally selected 4 of 11 systems in MCC's inventory as of October 23, 2024, for certain tests. We selected one system because it was MCC's only internal system and provided general support to other Agency systems, putting those other systems at risk if it is not secure. We selected three external systems based on an annual rotation plan to ensure that every system is regularly evaluated.

We conducted our review from September 2024 to December 2025 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Appendix A provides more detail on our scope and methodology.

Background

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 requires agency heads to implement policies and procedures to protect their information and

[1] For this evaluation, an effective information security program is defined as having an overall mature program based on the FY 2025 IG FISMA reporting metrics.

[2] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, version 2.0, April 3, 2025; and OMB and CIGIE, *FY 2025 FISMA Reporting Metrics Evaluator's Guide*, version 1.0, May 5, 2025.

information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

OMB and CIGIE provide instructions on assessing agency information security programs to inspectors general (IGs).[3] To help facilitate these assessments, the instructions contain metrics that IGs must evaluate for FY 2025.

Various requirements are in place to help MCC implement an effective information security program.

- OMB established minimum requirements for Federal information security programs and outlines agency responsibilities for the security of information and information systems.[4]
- The National Institute of Standards and Technology (NIST) issued requirements for Federal agencies managing cybersecurity risks in its framework. It also issued a catalog of security and privacy controls, which includes the need to perform security control assessments on information systems.[5] Additionally, NIST provides requirements for agencies to identify, assess, and mitigate cybersecurity risks throughout the supply chain at all levels of their organizations.[6]
- The IG FISMA reporting metrics included a requirement for agencies to consistently implement their policies and procedures for assessing and reviewing the supply chain-related risks associated with suppliers or contractors.
- MCC established procedures that detail the Agency's security authorization process for information systems and require security assessments to be performed every 12 to 18 months.[7]

MCC's chief information officer is responsible for overseeing the security posture of the Agency's information systems. The chief information officer is also responsible for establishing and implementing Agency policies to secure its systems from bad actors.

In our FY 2024 FISMA audit, our contracted audit firm concluded that MCC generally implemented an effective information security program.[8] However, the firm found a weakness in meeting event logging requirements that resulted in one recommendation to strengthen MCC's incident detection program. In addition, the firm found that MCC had not implemented

[3] OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, January 15, 2025; and OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, version 2.0, April 3, 2025.
[4] OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I: Responsibilities for Protecting and Managing Federal Information Resources, July 27, 2016; and OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, October 8, 2021.
[5] NIST, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication (SP) 800-53 (revision 5), September 2020.
[6] NIST, *Cybersecurity Supply Chain Risk Management Practices for Federal Information Systems and Organization*, SP 800-161, May 2022.
[7] MCC *Security Authorization and Assessment Procedure*, December 22, 2024.
[8] USAID OIG, *FISMA: Despite Challenges, MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2024* (A-MCC-24-001-C), August 22, 2024.

an FY 2023 recommendation to update the Agency's policies and procedures to reflect security controls identified in NIST's Special Publication 800-53, Revision 5.

MCC Implemented an Effective Information Security Program, but Concerns Exist With Supply Chain Policies and System Security Assessments

MCC implemented an effective information security program in FY 2025. However, we identified weaknesses related to supply chain policies and overdue security assessments for two of the four systems we reviewed. We also found that MCC implemented only two of four prior recommendations.

MCC Implemented an Effective Information Security Program in FY 2025

Our evaluation found that MCC implemented an effective information security program. For example, as required by OMB Circular A-130 and the FY 2025 IG FISMA reporting metrics, MCC:

- Maintained a centralized, enterprise-wide view of cybersecurity risk management activities across the organization.
- Maintained an accurate inventory of hardware and software assets.
- Implemented phishing-resistant multifactor authentication mechanisms for privileged and non-privileged users to access the organization's physical assets and information system.
- Implemented security controls to prevent unauthorized extraction of data from Agency systems and enhance network defenses, as required.
- Provided its personnel with awareness and specialized training that produced a demonstratable improvement in reducing the success of phishing attempts.

However, we found that MCC had not fully implemented its supply chain procedures or ensured that security assessments were performed for two key systems that contain important information pertaining to program performance, as required.

MCC Has Not Yet Fully Implemented Its Supply Chain Procedures

In response to a recommendation from our FY 2021 FISMA audit, MCC issued supply chain procedures for acquiring hardware and software for information and communications technology on June 11, 2025.[9] We found that the Agency has not fully implemented these procedures. An MCC official said the Agency's supply chain policies and procedures are implemented alongside the purchase of new IT systems, software, and tools. However, the

[9] *Supply Chain Risk Management Directive*, OCIO-Directive-03-ISSR-SR. We recommended that MCC develop and document supply chain policies, procedures, and strategies. See USAID OIG, *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (A-MCC-22-004-C), December 2, 2021.

official explained that procurement actions were put on hold or canceled due, in part, to the administration's ongoing foreign assistance review.[10] The hold and cancelation impacted MCC's ability to fully implement the procedures, which are tightly coupled with procurement. The official said MCC expects the procedures to be fully implemented by the end of calendar year 2025.

According to the FY 2025 IG FISMA reporting metrics, organizations should consistently implement their procedures for assessing and reviewing supply chain risks.[11] Further, NIST standards direct organizations to identify, assess, and mitigate cybersecurity risks throughout the supply chain at all levels of their organizations.[12]

Information technology equipment and software can be an entryway for hackers and foreign adversaries to access agency information systems and sensitive data contained in them. Supply chain procedures help ensure agencies buy from trusted sources and that purchased products do not have weaknesses that can be exploited. Fully implementing the procedures will better position MCC to mitigate threats from actors who can exploit supply chain vulnerabilities and compromise the confidentiality, integrity, or availability of the Agency's information systems. For example, in December 2020, several U.S. Federal agencies were impacted by a major supply chain cyberattack involving the network services provider SolarWinds. Malicious actors breached SolarWinds' development process and embedded harmful code into software updates, effectively creating covert access points within affected systems.

Given that sufficient time had not passed for MCC to fully implement its supply chain procedures and that MCC planned to fully implement them by the end of 2025, we are not making an associated recommendation and will continue to monitor MCC's progress.

MCC Did Not Ensure Security Assessments Were Performed for Two of Four Systems Reviewed

We found that MCC performed security assessments for two of four significant systems we reviewed, as required by its procedures and NIST guidance.[13] However, it did not ensure assessments were completed for the remaining two systems—one internal and one external system. For the internal system, MCC's procedures required the assessments to be performed

[10] On January 20, 2025, the President directed a pause on all U.S. foreign assistance for review. White House, Executive Order 14169, "Reevaluating and Realigning United States Foreign Aid," January 20, 2025.

[11] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, version 2.0, April 3, 2025.

[12] NIST, *Cybersecurity Supply Chain Risk Management Practices for Federal Information Systems and Organization*, SP 800-161, May 2022.

[13] For internal systems, the procedure states that, every 12–18 months, MCC will actively review and update at least 33 percent of the security controls listed in NIST, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53 (revision 5), September 2020, for every accredited information system. Based on these updates, the Agency is to grant approval to operate the system every 3 years. MCC, *Security Authorization and Assessment Procedure*, December 2024. For external systems, NIST SP 800-53, control CA-2 (d), states, "Assess the controls in the system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements."

every 12 to 18 months. According to NIST, agencies should define the frequency of security assessments for external systems and conduct those assessments accordingly.

MCC last performed a security assessment for the internal system in September 2023. Agency officials said they intentionally delayed the security assessment for the internal system because they planned to make major changes, including upgrading the system to Windows 11 and moving it to a data center. They explained that performing an assessment before a major change would not provide an accurate picture of the system's security and therefore would be wasteful. An Agency official said the Windows 11 upgrade had largely been completed, but the planned data center move was unexpectedly delayed due to the administration's foreign assistance review. This official estimated that barring any delays in awarding the data center contract, the data center move and the updated security assessment would be completed by the third quarter of FY 2026. Nevertheless, MCC did not have a detailed schedule for completing the assessment.

The Agency last performed a security assessment of the external system in May 2022. MCC contracts with an external provider to host and operate the system, which contains program performance data. However, our review found the contract did not require the provider to perform assessments or define how often assessments should be performed. Instead, the contract, which was due to end on August 31, 2025, only contained annual high-level requirements to provide security assurances to MCC.

A MCC official explained that the external system is unique in the Agency's IT system portfolio because it is contractor owned and operated rather than shared by several Federal agencies.[14] Therefore, the official said, MCC did not have a precedent or templates to work from when it developed security requirements for the system. OIG found that MCC also did not have procedures to incorporate security control assessments into contracts for external systems.

To mitigate risks related to the overdue security assessments, MCC officials said they had discussed a security control assessment report, which was in the final stages of completion, with the contractor and had reviewed plans to address identified system weaknesses. Further, based on their monitoring of both systems, they continued to authorize the systems to operate. Nevertheless, in addition to being noncompliant with requirements, by not conducting regular security assessments, MCC may have unidentified vulnerabilities, weaknesses, or gaps in its control measures. Thus, the Agency may be susceptible to cybersecurity threats and data breaches, putting sensitive data about American foreign investments at risk.

Further, MCC officials said they plan to issue a follow-on contract for the external system. As such, the Agency should have procedures for ensuring future contracts include appropriate information security requirements, such as the need for regularly scheduled security control assessments.[15]

[14] Such shared systems fall under the Federal Risk and Authorization Management Program, which is a government-wide initiative designed to provide a standardized approach for meeting security requirements.

[15] MCC, *Contracts Operating Manual*, Chapter 39, "Acquisition of Information Technology," May 2017, requires the Agency's chief information officer to approve IT acquisitions.

MCC Has Not Implemented Two of Four Prior OIG FISMA Recommendations

MCC implemented one open recommendation from our prior FISMA audits pertaining to supply chain policies and another pertaining to event logging requirements.[16] However, we found that the Agency did not implement a key recommendation to update its policies and procedures in compliance with NIST requirements for security controls and another to implement additional event logging requirements established by OMB.[17] Appendix B provides more detail on the status of our prior recommendations.

Conclusion

An effective information security program is essential to mitigate risks to MCC's systems and information. While MCC implemented an effective information security program in FY 2025, implementing additional controls will help the Agency manage its supply chain and security assessments more effectively. Moreover, strengthening these controls will put the Agency in a better position to protect the confidentiality, integrity, and availability of its information systems and sensitive data contained in them. By taking steps to address identified weaknesses, MCC will better protect its information systems from cyberattacks and other security risks, ultimately protecting Americans, government resources, and sensitive operating data from disruptive bad actors.

Recommendations

We recommend that MCC's Chief Information Officer take the following actions:

1. Develop a schedule for completing the overdue security assessment of the internal system and conduct the assessment accordingly.
2. Develop and implement procedures requiring contracts for external systems to include assessments of security controls at a frequency MCC defines.

[16] Recommendation 2, USAID OIG, *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA*, (A-MCC-22-004-C), December 2, 2021; and Recommendation 3, USAID OIG, *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (A-MCC-23-002-C), September 5, 2023.

[17] Recommendation 1, USAID OIG, *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (A-MCC-23-002-C), September 5, 2023; and Recommendation 1, USAID OIG, *FISMA: Despite Challenges, MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2024* (A-MCC-24-001-C), August 22, 2024.

OIG Response to Agency Comments

We provided our draft report to MCC on December 11, 2025. On January 7, 2026, we received the Agency's response, which is included in Appendix C of this report.

The report included two recommendations, and MCC agreed with both. We acknowledge management decisions on both recommendations and consider them resolved but open pending completion of planned activities.

Appendix A. Scope and Methodology

We conducted our work from September 2024 through December 2025 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Our objective was to determine whether MCC implemented an effective information security program.

We focused on MCC's information security program for FY 2025 through July 24, 2025, the date we submitted the final IG FISMA reporting metrics to OMB with one exception: we reviewed the Agency's supporting documentation for one prior recommendation after that date. We conducted our work at MCC's headquarters in Washington, DC.

To answer our objective, we followed the FY 2025 IG FISMA reporting metrics and FISMA Evaluator's Guide, which provides a baseline of suggested evidence and test steps for FISMA-related evaluations. To assess the effectiveness of MCC's information security program, we also used criteria referenced throughout the metrics, including NIST's Cybersecurity Framework, security and privacy control guidance, OMB Circular A-130, and supply chain risk management practices.[18] In addition, we used MCC policies and procedures to assess its implementation of certain controls.[19]

We judgmentally selected 4 of 11 systems in the Agency's inventory as of October 23, 2024, for tests of the 6 functional areas in NIST's Cybersecurity Framework. We selected one system because it is MCC's only internal system, provides general support to other Agency systems, and will put other systems at risk if it is not secure. We selected three external systems based on an annual rotation plan to ensure that every system is regularly evaluated. The results and conclusions we drew from our sample are limited to the systems we reviewed and cannot be projected to the entire population of systems. However, we determined that our method for selecting these systems was appropriate for the objective of our evaluation and that the selection would generate valid, reliable evidence to support our findings and conclusions.

We reviewed MCC's hardware inventory, evidence of hardware scans, and evidence of monthly hardware audits to determine the extent to which MCC maintained a current inventory of hardware with the detailed information necessary for tracking and reporting, as required by OMB Circular A-130. In addition, we reviewed MCC's supply chain policy and interviewed MCC officials to determine whether its supply chain policies and procedures had been implemented.[20]

We reviewed results of vulnerability scans and Change Control Board meetings to determine the extent to which MCC used flaw remediation processes, including vulnerability scanning and patch management, to address vulnerabilities on the network, as required by NIST guidance.[21]

[18] NIST, *The NIST Cybersecurity Framework (CSF)*, version 2.0, February 26, 2024; NIST, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53 (revision 5), September 2020; and NIST, *Cybersecurity Supply Chain Risk Management Practices for Federal Information Systems and Organization*, SP 800-161, May 2022.

[19] MCC, *Information System Security Policy*, February 2, 2021, and *Security Authorization and Assessment Procedure*, December 2, 2024.

[20] MCC, *Supply Chain Risk Management Directive*, June 11, 2025.

[21] The Change Control Board reviews and approves proposed changes in MCC's IT systems. MCC, *Configuration Management Procedure*, December 27, 2022.

We also reviewed system authorizations and the most recent security control assessment reports for the four systems in our sample to determine the extent to which MCC performed ongoing information system assessments to grant system authorizations, as required by MCC's procedures and NIST.[22] Further, we reviewed incident event monitoring dashboards, event logs, and log retention settings to determine the extent to which MCC implemented processes related to incident detection and analysis, as required by OMB Memorandum 22-01 and NIST.[23]

We interviewed MCC officials to learn about the policies and procedures MCC has in place for its information security program. Additionally, we reviewed legal requirements stipulated in FISMA.

To determine the status of recommendations we made to MCC in our FY 2021, FY 2023, and FY 2024 FISMA audit reports, we reviewed the Agency's closure requests and supporting documentation where received. Appendix B provides additional detail on these recommendations.

[22] MCC, *Security Authorization and Assessment Procedure*, December 2, 2024; MCC, *Information Security Continuous Monitoring (ISCM) Strategy and Procedures*, December 9, 2024; and NIST, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53 (revision 5), September 2020.

[23] OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, October 8, 2021; and NIST, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53 (revision 5), September 2020.

Appendix B. Status of Prior Recommendations

The following table provides the status of recommendations from our FY 2021, FY 2023, and FY 2024 FISMA audit reports that were open as of October 1, 2024, the beginning of the period of our evaluation.[24]

Table 1. Prior OIG Recommendations

Report & Recommendation #	Recommendation	MCC's Position	Evaluator's Position
A-MCC-22-004-C (FY 2021, Rec. 2)	We recommend that MCC's chief information officer develop and document supply chain policies, procedures, and strategies.	Open	Closed*
A-MCC-23-002-C (FY 2023, Rec. 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.	Open	Open
A-MCC-23-002-C (FY 2023 Rec. 3)	We recommend that MCC's chief information officer implement level 2 event logging requirements in accordance with Office of Management and Budget memorandum M-21-31.	Closed	Closed
A-MCC-24-001-C (FY 2024, Rec. 1)	We recommend that MCC's chief information officer implement level 3 event logging requirements in accordance with Office of Management and Budget Memorandum M-21-31.	Open	Open

* Based on our FY 2025 FISMA assessment, MCC has taken the recommended actions.
Source: OIG's FY 2021, 2023, and 2024 FISMA audit reports and assessment of MCC's recommendation closure requests and supporting documentation.

[24] USAID OIG, *MCC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA*, (A-MCC-22-004-C), December 2, 2021; USAID OIG, *MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2023 in Support of FISMA* (A-MCC-23-002-C), September 5, 2023; and USAID OIG, *FISMA: Despite Challenges, MCC Generally Implemented an Effective Information Security Program for Fiscal Year 2024* (A-MCC-24-001-C), August 22, 2024.

Appendix C. Agency Comments

MILLENNIUM
CHALLENGE CORPORATION
UNITED STATES OF AMERICA

DATE: January 7, 2026

TO: Gabriele A. Tonsil
Acting Assistant Inspector General for Audit, Inspections, and Evaluations
Office of the Inspector Gener, United States Agency for International Development

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

SUBJECT: MCC's Management Response to the Draft Audit Report, *FISMA: MCC Implemented an Effective Information Security Program for FY 2025 Despite Some Concerns*

The Millennium Challenge Corporation (MCC) appreciates the opportunity to review the draft report on the Office of Inspector General's (OIG) audit, *FISMA: MCC Implemented an Effective Information Security Program for FY 2025 Despite Some Concerns*. 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).

Recommendation 1 – Develop a schedule for completing the overdue security awareness of the internal system and conduct the assessment accordingly.

MCC Management Response: MCC concurs with this recommendation. MCC will develop the schedule by May 8, 2026.

Recommendation 2 – Develop and implement procedures requiring contracts for external systems to include assessments of security controls at a frequency MCC defines.

MCC Management Response: MCC concurs with this recommendation. MCC will develop and implement the procedures by September 30, 2026.

If you have any questions or require any additional information, please contact me at 202-521-2652 or icece@mcc.gov; or Lori Giblin, Chief Risk Officer at giblinlm@mcc.gov.

CC: Khadija Walker, Deputy Assistance Inspector General for Audits, Evaluations, and Inspections, OIG, USAD
Lisak Banks, Audit Director, OIG, USAID
Felix Adenusi, POC Auditor and Assistant Director, OIG, USAID
Alberto Calimano-Colon, Lead Auditor and COR, OIG, USAID
Mark Norman, Auditor and ACOR, OIG, USAID
Abdel Maliky, Acting Vice President and CFO, MCC
Kelci Ibrahim, Acting Managing Director FMD, MCC
Julio Mercado, CISO, MCC
Lori Giblin, Chief Risk Officer, MCC

Visit our website at oig.usaid.gov and
follow us on social media.

X: @AidOversight
LinkedIn: USAID Office of Inspector General
Instagram: @usaid.oig

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

Report Waste, Fraud, and Abuse
Online Complaint Form