OFFICE OF INSPECTOR GENERAL

U.S. International Development Finance Corporation

Fiscal Year 2025 DFC Federal Information Security Modernization Act of 2014 Performance Audit

October 9, 2025

Audit Report DFC-25-005-C

1100 New York Avenue, NW
Washington, DC 20527
https://www.dfc.gov/oig

Report Highlights

Office of Inspector General
International Development Finance Corporation

Fiscal Year 2025 DFC Federal Information Security Modernization Act of 2014 Performance Audit

What Was Reviewed

The U.S. International Development Finance Corporation Office of Inspector General contracted with the independent public accounting firm RMA Associates, LLC (RMA) to conduct the *Federal Information Security Modernization Act of 2014* (FISMA) Performance Audit of the United States International Development Finance Corporation (DFC) for Fiscal Year (FY) 2025 to evaluate the effectiveness of the DFC's information security program and practices, and determine what maturity level DFC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2025 Inspectors General (IG) FISMA Reporting Metrics v2.0* (April 2025).

Our objective was to evaluate the effectiveness of the DFC's information security program and practices and determine the maturity level DFC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2025 IG FISMA Reporting Metrics v2.0* (April 2025).

What Was Found

In this Performance Audit of DFC, RMA determined that DFC's information security program and practices were effective for FY 2025, as DFC's information security program met the criteria required to be assessed at a maturity level of Managed and Measurable (Effective). RMA's tests of the information security program identified two findings that fell within the data protection and privacy and information security continuous monitoring domains.

Recommendation

We made four recommendations to DFC's Chief Information Officer to address the two findings and help further strengthen DFC's information security program. Specifically, we recommended that DFC's Chief Information Officer:

- **Recommendation 1**: Periodically perform a physical inventory of all mobile devices, including those pending disposal, to ensure all assets are accounted for and accurately reflected in the asset tracking system.

- **Recommendation 2**: Assign assessors to perform tests of effectiveness on all DFC's System Security Plan with a sufficient degree of independence in accordance with National Institute of Standards and Technology Special Publication 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations, Revision 5.1.1.
- **Recommendation 3**: Document the independence of the assessment team in the risk assessment, including organizational relationships, contract structures, if applicable, and oversight arrangements.
- **Recommendation 4**: Ensure the risk assessment is reviewed and approved by an Authorizing Official prior to the commencement of any assessment activity.

Office of Inspector General
U.S. International Development Finance Corporation

MEMORANDUM:

Date: October 9, 2025

To: Mr. Willie Williams
Acting, CHIEF INFORMATION OFFICER (CIO)

From: Ms. Erika Ersland ERIKA ERSLAND Digitally signed by ERIKA ERSLAND Date: 2025.10.09 15:36:44 -04'00'
Acting, Assistant Inspector General for Audit

Subject: Fiscal Year 2025 DFC Federal Information Security Modernization Act of 2014 Performance Audit (Report Number DFC-25-005-C)

The Office of Inspector General contracted with the independent public accounting firm of RMA Associates, LLC (RMA) to conduct the *Federal Information Security Modernization Act of 2014* (FISMA) Performance Audit of the United States International Development Finance Corporation (DFC) for Fiscal Year (FY) 2025 to evaluate the effectiveness of the DFC's information security program and practices, and determine what maturity level DFC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2025 Inspectors General (IG) FISMA Reporting Metrics v2.0* (April 2025). The contract required RMA to perform the engagement in accordance with generally accepted government auditing standards, Office of Management and Budget, *FY 2025 IG FISMA Reporting Metrics v2.0*, and Circular No. A-130, Section 522 of the Consolidated Appropriations Act of 2005, and others, such as the National Institute of Standards and Technology (NIST).

In its Performance Audit of DFC, RMA reported the information security program and practices were effective for FY 2025, as DFC's information security program met the criteria required to be assessed at a maturity level of Managed and Measurable (Effective). RMA's tests of the information security program identified two findings that fell within the data protection and privacy and information security continuous monitoring domains.

RMA is responsible for the attached auditor's report dated September 11, 2025, and the conclusions expressed therein. We do not express opinions on DFC's information systems or internal control over information systems, or on whether DFC's information systems complied with FISMA, or draw conclusions on compliance and any other matters.

CC: Acting Chief Executive Officer
Chief of Staff
Chief Administrative Officer
Chief Financial Officer
Senior VP Operations

Chief Information Security Officer
Administrative Counsel
Managing Director Office of Financial and Portfolio Management
RMA Associates

RMA Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

United States International Development Finance Corporation

Federal Information Security Modernization Act of 2014

Performance Audit Report for Fiscal Year 2025

RMA | Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone : (571) 429-6600
www.rmafed.com

September 11, 2025

Naga Jujjavarapu, Acting Deputy Inspector General
Office of Inspector General
United States International Development Finance Corporation
1100 New York NW
Washington, DC 20527

Re: United States International Development Finance Corporation Federal Information Security Modernization Act of 2014 Audit Report for Fiscal Year 2025

Dear Ms. Jujjavarapu:

RMA Associates, LLC is pleased to submit our performance audit report on the effectiveness of the United States International Development Finance Corporation's (DFC) information security program and practices for Fiscal Year (FY) 2025. In accordance with the *Federal Information Security Modernization Act of 2014* (FISMA), the objective of this performance audit was to evaluate the effectiveness of the DFC's information security program and practices and determine the maturity level DFC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2025 Inspectors General (IG) FISMA Reporting Metrics v2.0*. The performance audit fieldwork covered DFC's headquarters in Washington, DC, from February 3, 2025, to August 1, 2025.

Based on the results of our performance audit, we determined that DFC's information security program and practices were effective for FY 2025, as the criteria assessed for DFC's information security program met the maturity level of Managed and Measurable. Our assessment of the information security program identified two findings that fell within the data protection and privacy and information security continuous monitoring domains. We made four recommendations to assist DFC in strengthening its information security program. Further, one prior FISMA performance audit recommendation remains open.

Our report includes **Appendices I**: Status of Prior Year Recommendations, **II**: Management Responses, **III**: Evaluation of Management Responses, and **IV**: Glossary of Acronyms. Further details of our findings and recommendations are included in the accompanying report.

We conducted this performance audit 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The performance audit included an assessment of DFC's information security program and practices consistent with FISMA and reporting instructions issued by the Office of Management and Budget (OMB). We considered the guidelines established by the OMB, Department of Homeland Security (DHS), and National Institute of Standards and Technology (NIST). We assessed four internal and external systems out of the four FISMA reportable systems from DFC's FISMA inventory of information systems.

For FY 2025, OMB required Inspector Generals to assess 25 metrics from *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, including both core and supplemental metrics. These metrics are coordinated and agreed upon by the Council of the Inspectors General on Integrity and Efficiency, the Chief Information Security Officer, OMB, and the Cybersecurity & Infrastructure Security Agency. This approach is aligned with NIST *Cybersecurity Framework* 2.0, which underscores the essential role of governance in managing cybersecurity risks and integrating cybersecurity into an organization's overall enterprise risk management strategy. The FY 2025 IG Metrics were aligned with the following Cybersecurity Framework function areas: Govern, Identify, Protect, Detect, Respond, and Recover to determine the effectiveness of agencies' information security programs. The *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, classifies information security programs and practices into five maturity levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

We have also prepared responses to the OMB's M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* guidance, encouraging agencies to shift towards a continuous assessment process for their annual independent assessment using *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, and the submission of evaluations via CyberScope. These metrics provide reporting requirements across function areas to be addressed in the independent assessment of agencies' information security programs.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. We caution that projecting the results of our performance audit to future periods is subject to the risk that conditions may significantly change from their current status. The information included in this report was obtained from DFC on or before August 1, 2025. We have no obligation to update our report or to revise the information contained therein to reflect events occurring after August 1, 2025.

We greatly appreciate the opportunity to serve your organization and the assistance provided by your staff and the DFC. We will be happy to answer any questions you may have concerning the report.

Sincerely,

RMA Associates

RMA Associates, LLC
Arlington, VA

Table of Contents

Introduction

This report presents the results of RMA Associates, LLC (RMA) 's independent performance audit of the United States International Development Finance Corporation (DFC) 's information security program and practices. The *Federal Information Security Modernization Act of 2014* (FISMA)[1] requires Federal agencies to conduct an annual independent evaluation to assess their information security program and practices to determine the effectiveness of such programs and practices and to report the results of the audits to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) to collect annual FISMA responses.

DFC's Office of Inspector General (OIG) engaged RMA to conduct an annual performance audit of DFC's information security program and practices supporting the FISMA performance audit requirement. The objective of this performance audit was to evaluate the effectiveness of DFC's information security program and practices and determine the maturity level DFC achieved for each of the core metrics and Fiscal Year (FY) 2025 supplemental metrics outlined in the *FY 2025 Inspectors General (IG) FISMA Reporting Metrics v2.0*, dated April 2025.

As part of our performance audit, we responded to the FY 2025 20 core and five supplemental metrics specified in OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 2025.[2] These metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs.[3] We also considered applicable DFC and OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards, where applicable.

Background

United States International Development Finance Corporation

DFC helps bring private capital to the developing world. It was created by the *Better Utilization of Investments Leading to Development Act of 2018,* which authorized DFC until October 2025 (seven years). DFC began operations in January 2020, consolidating the functions of its predecessor agencies, the Overseas Private Investment Corporation, and the U.S. Agency for International Development's Development Credit Authority.

DFC, the U.S. Government's development finance institution, partners with the private sector to finance solutions to the most critical challenges facing today's developing world. DFC invests across energy, healthcare, critical infrastructure, and technology sectors. DFC also provides financing for small businesses and women entrepreneurs to create jobs in emerging markets and

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).
[2] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the Inspector General FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council.
[3] Refer to the section titled, *Objective, Scope, and Methodology,* for more details.

supports projects in various industries from critical infrastructure to power generation, healthcare, agriculture, technology, and financial services.

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*, required each Federal agency to develop, document, and implement an agency-wide program to provide security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. FISMA amended the *Federal Information Security Management Act of 2002* and provided several modifications that modernize Federal security practices to address evolving security concerns. These changes resulted in less overall reporting, strengthened the use of continuous monitoring in systems, and increased focus on the agencies for compliance and reporting that is more concentrated on the issues caused by security incidents.

FISMA, along with the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996* (also known as the Clinger-Cohen Act), explicitly emphasizes a risk-based approach to cost-effective security. In support of and reinforcing this legislation, OMB, through Circular No. A-130, *Managing Information as a Strategic Resource*, requires executive agencies within the Federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibilities;
- Periodically review the security controls in its systems; and
- Authorize system processing prior to operations and periodically after that.

These management responsibilities presume that responsible agency officials understand the risks and other factors that could adversely affect the organization's missions. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information and systems, and make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct day-to-day operations and accomplish its stated mission with adequate security, or security commensurate with the risk, including the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information.

FISMA provided OMB with oversight authority over agency security policies and practices and authorized the implementation of agency policies and practices for information systems to DHS.[4]

FISMA required the Secretary of DHS to develop and oversee the implementation of operational directives that require agencies to implement OMB standards and guidelines for safeguarding Federal information and systems from known or reasonably suspected information security threats,

[4] FISMA, Pub. L. No. 113-283, 128 Stat. 3073, December 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2521.

vulnerabilities, or risks. FISMA directed the Secretary to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security standards.[5] FISMA authorized the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.[6]

Additionally, FISMA directed Federal agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the U.S. Government Accountability Office. The reports are required to include: (1) threats and threat actors, vulnerabilities, and impacts of the incidents; (2) risk assessments of affected systems before the incidents; (3) the status of system compliance at the time of the incidents; (4) detection, response, and remediation actions; (5) total number of incidents; and (6) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.[7]

Key Changes to the FY 2025 IG FISMA Metrics

One of the goals of the annual FISMA audits is to assess agencies' progress toward achieving objectives that strengthen Federal cybersecurity. The IG FISMA Reporting Metrics have been updated to determine agency progress in achieving the objectives, as follows:

- NIST *Cybersecurity Framework 2.0*: NIST published Cybersecurity Framework (CSF) Version 2.0, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy. A new IG FISMA function area (Govern) was created that includes a new domain (Cybersecurity Governance). In addition, new supplemental metrics were designed to assess the maturity of an organization's:
  - Use of cybersecurity profiles to understand, tailor, assess, prioritize, and communicate cybersecurity objectives.
  - Cybersecurity risk management strategy, which establishes an organization's priorities, constraints, risk tolerance, and appetite statements and is used to support operational risk decisions.
  - Processes and authorities to foster cybersecurity accountability, performance assessment, and continuous improvement.

In addition, to align with the CSF 2.0, the supply chain risk management (SCRM) domain was moved from the Identify function area to the Govern function area and renamed to Cybersecurity SCRM (C-SCRM) to better reflect the cybersecurity environment. Furthermore, a new domain in the Identify function area (Risk and Asset Management) was established to group metrics on system inventory and hardware, software, and data management.

[5] Ibid.
[6] Ibid.
[7] Ibid.

- **Zero Trust Architecture (ZTA) Implementation**: The FY 2025 metrics included two new supplemental metrics critical to achieving ZTA objectives. These new metrics assess the maturity of an organization's (1) data management capabilities, and (2) ability to monitor and measure the integrity and security posture of all owned and associated assets.
- **Supplemental metrics for FY 2025**: Five supplemental metrics, including metric numbers 1, 2, 3, 10 and 27, were in scope for the FY 2025 IG FISMA audit.
- **Information System Level Risk Management**: The core metric on information system level risk management (Metric 11, formerly Metric 5) was revised to focus on the maturity of agencies' implementation of the NIST risk management framework.

For FY 2025, the IG audit had a deadline of August 1, 2025, for FISMA reporting to OMB and the DHS. This allowed agencies more time to incorporate the necessary changes identified by the IG audits in their budget submissions.

Core and FY 2025 Supplemental IG Metrics

OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, specified the FY 2025 20 Core and five Supplemental IG Metrics. It directed IGs to report the assessed maturity levels of these metrics in CyberScope[8] no later than August 1, 2025. The FY 2025 FISMA IG Metrics were aligned with the six function areas in the NIST *Cybersecurity Framework 2.0* as follows:

- Govern, includes metrics pertaining to Cybersecurity Governance and Cybersecurity Supply Chain Risk Management;
- Identify, includes metrics pertaining to Risk and Asset Management;
- Protect, includes metrics pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
- Detect, includes metrics pertaining to Information Security Continuous Monitoring (ISCM);
- Respond, includes metrics pertaining to Incident Response; and
- Recover, includes metrics pertaining to Contingency Planning.

We assessed the effectiveness of information security programs and practices on a maturity model spectrum, in which the foundation levels ensure the development of sound policies and procedures. The FY 2025 IG Metrics classifies information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Within the context of the maturity model, Level 4 (Managed and Measurable) and Level 5 (Optimized) represent an effective level of security. Table 1: IG Audit Maturity Levels explains the five maturity model levels.

[8] CyberScope is a web-based platform to streamline the reporting of information security practices required under FISMA. As mandated by OMB and DHS, federal agencies must collect FISMA performance metrics data and upload the results into CyberScope.

Table 1: IG Audit Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies were not formalized; activities were performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies were formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies were consistently implemented, but quantitative and qualitative effectiveness measures were lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures of the effectiveness of policies, procedures, and strategies were collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies were fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

For FY 2025, IGs continued to focus on a calculated weighted average approach, wherein the average of the metrics in a particular domain was used by IGs to determine the effectiveness of individual function areas (govern, identify, protect, detect, respond, and recover) and the overall program. To provide IGs with additional flexibility and encourage evaluations based on agencies' risk tolerance and threat models, calculated averages were not automatically rounded (i.e., rounded up or down based on mathematical rules) to a particular maturity level. In the FY 2025 calculated average scoring model, core metrics and supplemental metrics were calculated independently to determine a domain's maturity calculation and provide data points for assessing program and function area effectiveness. For example, if the calculated core metric maturity of two of the function areas is Level 3 (Consistently Implemented) and the calculated core metric maturity of the remaining three function areas is Level 4 (Managed and Measurable), then the information security program rating would average a 3.60.[9]

We focused on the results of the core metrics to determine maturity levels. We used the calculated averages of the supplemental metrics as a data point to support our risk-based determination of overall program and function level effectiveness. The DHS computed average of the maturity level was 4.27, the Managed and Measurable level. As a result, DFC's overall assessed maturity level was effective.

DFC's FY 2025 calculated core metric, supplemental metric, assessed maturity averages, and assessed maturity level by function are presented in Table 2: Overall Calculated Averages Maturity Calculation in FY 2025**.**

[9] *FY 2025 IG FISMA Reporting Metrics v2.0*, April 3, 2025.

Table 2: Overall Calculated Averages Maturity Calculation in FY 2025

Function	Core Metrics	Supplemental Metrics	Assessed Maturity Average[10]	Assessed Maturity
Govern[11]	5.00	3.67	3.86	Managed and Measurable
Identify	4.60	4.00	4.60	Managed and Measurable
Protect	4.50	N/A	4.50	Managed and Measurable
Detect	4.00	4.00	4.00	Managed and Measurable
Respond	4.00	N/A	4.00	Managed and Measurable
Recover	4.50	N/A	4.67	Managed and Measurable
Overall Maturity	**4.43**	**3.89**	**4.27**	**Managed and Measurable**

Summary Performance Audit Results

We determined that, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the DFC's information security program and practices were established and maintained for the six NIST Cybersecurity Framework functions[12] and 10 FISMA Metric Domains.[13] The overall maturity level of the DFC's information security program was determined as Managed and Measurable, as described in this report. Accordingly, we determined DFC's information security program and practices were effective for FY 2025.

We provided the DFC with a draft of this report for their review and comment. In a written response, management agreed with the results of our performance audit and indicated in subsequent correspondence that the target completion date for recommendations (refer to Appendix II: Management Response for the DFC's response in its entirety, and Appendix III: Evaluation of Management Response for our assessment of management's response).

During FY 2025, DFC had not resolved the single open recommendation from the FY 2024 FISMA audit. Appendix I: Status of Prior Year Findings provides a summary of the status of recommendations from the prior year.

We identified weaknesses in DFC's security posture in preserving the agency's information and the confidentiality, integrity, and availability of its information systems. Consequently, we noted

[10] The FY 2025, the assessed maturity average was computed by averaging the core and supplemental metrics and the calculated averages were not rounded to determine the maturity level. In determining maturity levels and the overall effectiveness of DFC's information security program, RMA focused on the results of the core metric and made a risk-based assessment of overall program and function level effectiveness.

[11] The Govern function area was introduced in FY 2025

[12] OMB, DHS, and CIGIE developed the FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The 10 FISMA Metric Domains were aligned with the six functions: (1) govern, (2) identify, (3) protect, (4) detect, (5) respond, and (6) recover as defined in the NIST *Cybersecurity 2.0*.

[13] As described in the FISMA Reporting Metrics, the 10 FISMA Metric Domains are: (1) Cybersecurity Governance, (2) Cybersecurity Supply Chain Risk Management, (3) Risk and Asset Management, (4) Configuration Management, (5) Identity and Access Management, (6) Data Protection and Privacy, (7) Security Training, (8) Information Security Continuous Monitoring, (9) Incident Response, and (10) Contingency Planning.

weaknesses in two IG FISMA Metric Domains: DFC lacked historical traceability and accountability for mobile devices, and DFC did not ensure the independence of the Security Assessor. We made four recommendations to assist DFC in strengthening its information security program. Nonetheless, we determined that DFC implemented an effective information security program, considering the agency's unique mission, resources, and challenges.

The maturity level for the 10 domains is presented below in Table 3: DFC's FY 2025 Maturity Levels:

Table 3: DFC's FY 2025 Maturity Levels

Function	Maturity Level	Overall Maturity Level
Function 1: Govern	• Cybersecurity Governance—Consistently Implemented (Level 3) • Cybersecurity Supply Chain Risk Management— Optimized (Level 5)	Managed and Measurable (Level 4)
Function 2: Identify	Risk and Asset Management	Managed and Measurable (Level 4)
Function 3: Protect	• Configuration Management—Managed and Measurable (Level 4) • Identity Management—Optimized (Level 5) • Data Protection and Privacy—Consistently Implemented (Level 3) • Security Training—Optimized (Level 5)	Managed and Measurable (Level 4)
Function 4: Detect	Information Security—Continuous Monitoring	Managed and Measurable (Level 4)
Function 5: Respond	Incident Response	Managed and Measurable (Level 4)
Function 6: Recover	Contingency Planning	Managed and Measurable (Level 4)
	Overall	**Managed and Measurable (Level 4)**
	Overall	**Effective**

The following paragraphs provide more details on each domain's assessed maturity level and offer recommendations to the Chief Information Officer to remediate deficiencies.

Cybersecurity Governance

We determined the DFC's overall maturity level for the Cybersecurity Governance program was Consistently Implemented.

Testing performed by RMA's independent auditors found that DFC had identified its current cybersecurity profiles in alignment with the CSF 2.0 and was in the process of developing and finalizing its target cybersecurity profile, which takes into account anticipated changes to the organization's cybersecurity posture. Therefore, DFC did not assess the gaps between its current and target profiles and has not created and implemented a prioritized action plan. However, DFC implemented its risk management strategy, evaluating and adjusting it based on its threat environment and agency-wide cyber and privacy risk assessments. Roles, responsibilities, and authorities related to cybersecurity risk management were established and communicated. Stakeholders were held accountable for carrying out their roles and responsibilities effectively. Although the assessed maturity level for the agency's Cybersecurity Governance program was Consistently Implemented, based on DFC's overall implementation of security controls and considering the unique mission, resources, and challenges of DFC, RMA concluded that DFC's cybersecurity governance controls in place were overall effective.

Cybersecurity Supply Chain Risk Management

We determined the DFC's overall maturity level for the C-SCRM program was Optimized.

DFC developed and implemented a C-SCRM strategy, policies, and procedures to manage supply chain risks with suppliers, contractors, and systems. Additionally, DFC monitored and analyzed both qualitative and quantitative performance measures to assess the effectiveness of its C-SCRM strategy. DFC also obtained sufficient assurance through audits, test results, or other forms of evaluation that the security and supply chain controls of systems or services provided by contractors meet FISMA requirements, OMB policy, and applicable NIST guidance. Testing performed by the independent auditors found no exceptions for the C-SCRM program, and the controls were operating as intended. We determined that DFC's C-SCRM controls in place were overall effective.

Risk and Asset Management

We determined the DFC's overall maturity level for the Risk and Asset Management program was Managed and Measurable.

DFC implemented its security architecture across the enterprise, business process, and system levels to help leadership make informed decisions regarding risk management. Those risk management decisions helped improve and update DFC's risk management policies, procedures, and strategy, including methodologies for categorizing risk, developing a risk profile, assessing risk, determining risk appetite/tolerance levels, responding to risk, and monitoring risk. Additionally, DFC captured and shared lessons learned on the effectiveness of risk management processes and activities to update the program. Information systems, hardware, and software assets inventory were maintained comprehensively and accurately. Furthermore, DFC utilized automated systems to monitor the lifecycle of hardware assets connected to the network, including mobile devices. These assets were managed to align with agency standards before network integration. DFC consistently maintained a comprehensive and accurate inventory of its data and corresponding metadata for each data type, ensuring that the data and metadata in its inventories were subject to the monitoring processes defined within the DFC's ISCM strategy. Testing performed by the independent auditors found no exceptions for risk management, and the controls were operating as intended. Consequently, based on DFC's overall implementation of security controls and considering the unique mission, resources, and challenges of DFC, we determined that DFC's Risk and Asset Management controls in place were overall effective.

Configuration Management

We determined the DFC's overall maturity level for the Configuration Management program was Managed and Measurable.

DFC implemented an organization-wide configuration management plan, which was integrated into its risk management and continuous monitoring processes. DFC monitored, analyzed, and reported qualitative and quantitative performance measures on the effectiveness of its change control activities and documented lessons learned on the effectiveness of its change control activities. DFC managed both code-based and configuration-based vulnerabilities by utilizing their security software scanning tools on all systems by providing scan reports. In addition, DFC utilized various automated mechanisms to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact and mitigate the spike in vulnerabilities. Although outstanding vulnerabilities were found during their internal scans, we determined the overall risk is low. This was because DFC had appropriate technical controls in place to manage and mitigate any potential spike in vulnerabilities.

Additionally, due to the nature of DFC's operations, where employees frequently travel and devices are often offline, patching may be delayed. The vulnerabilities were automatically addressed as soon as the laptops were powered on and reconnected to the network. Testing performed by the independent auditors found no exceptions for the Configuration Management program, and the controls were operating as intended. We determined that DFC's Configuration Management controls in place were overall effective.

Identity and Access Management

We determined the DFC's overall maturity level for the Identity and Access Management program was Optimized.

DFC ensured that its processes for provisioning, managing, and reviewing privileged accounts were consistently implemented across the organization. Additionally, DFC implemented multi-factor authentication mechanisms for both privileged and non-privileged users of the organization's physical and logical assets. DFC implemented a third-party identity management cloud service for its enterprise-wide single sign-on solution. All of DFC's systems interface with the solution to oversee employees, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on the effectiveness in near real-time. DFC's implementation of its single sign-on solution and integration with [redacted] demonstrated that DFC employed automated mechanisms to manage privileged accounts, including the automatic removal of temporary, emergency, and inactive accounts.

Additionally, DFC utilized lessons learned, end users' devices were properly configured, and privileged users utilized a strong authentication mechanism. Testing performed by the independent auditors found no exceptions for the Identity and Access Management program, and the controls were operating as intended. We determined that DFC's Identity and Access Management controls in place were overall effective.

Data Protection and Privacy

We determined the DFC's overall maturity level for the Data Protection and Privacy program was Consistently Implemented. We identified one weakness in the Data Protection and Privacy domain related to the lack of historical traceability and accountability for mobile devices.

DFC Lacked Historical Traceability and Accountability for Mobile Devices

According to NIST Special Publication (SP) 800-53 Revision 5.1.1 *Security and Privacy Controls for Information Systems and Organizations,* CM-8 System Component Inventory, it requires organizations to create and maintain a detailed inventory of all system components—hardware, software, and firmware—that accurately represents the system, avoids duplication, and provides enough detail for accountability, such as system names, owners, versions, specifications, licenses, and network details. This inventory must be reviewed and updated at an organization-defined frequency and may be managed centrally, provided system-specific details are included. Effective accountability also involves documenting acquisition details, such as cost, model, serial number, and location. In addition, in alignment with the Green Book, management must ensure proper documentation and records, and design information technology (IT) control activities that ensure the completeness, accuracy, and validity of information processing.

From a population of 967 mobile devices, 112 devices (12%) were recorded as pending disposal on the inventory sheet titled "Mobile Device Inventory." We selected a sample of 10 devices from 112 to determine whether they existed. DFC was unable to locate eight of the 10 sampled devices.

DFC management stated that DFC's older phones (mobile devices) did not have external serial numbers and were not tagged or recorded into an asset tracking system. As a result, DFC had no verifiable traceability between devices and historical inventory records. A new asset tagging process was implemented in September/October 2024, and older phones have since been retroactively tagged and updated in a cloud-based software tool with a "pending disposal" status. However, some of the older phones could not be tagged because they were [redacted] and inaccessible.

Improper reporting of DFC records may result in misallocation or loss of mobile devices. Devices that are untracked or untagged may still contain sensitive data. If lost or stolen, this data could be compromised, especially if the devices are not properly wiped or encrypted. Additionally, if an iPhone is misplaced or stolen, DFC may not become aware of the incident in a timely manner. This delay in detection increases the risk that sensitive data could be accessed or misused before appropriate protective actions can be taken.

Recommendation 1: We recommend that DFC's Chief Information Officer periodically perform a complete physical inventory of all mobile devices, including those pending disposal, to ensure all assets are accounted for and accurately reflected in the asset tracking system.

RMA also noted that DFC's systems were approved to collect and process Personally Identifiable Information (PII). The controls over PII were the responsibility of DFC's outsourced service providers. Therefore, DFC monitored and analyzed quantitative and qualitative performance measures on the effectiveness of its privacy activities and used the information to make necessary adjustments to reach the managed and measurable level. DFC conducted an independent review of its privacy program and [redacted] Furthermore, DFC participated in a [redacted] and applied the lessons learned to enhance the Data Breach Response Plan, as necessary. Testing performed by the independent auditors found one exception for data protection and privacy. We determined that the DFC's data protection and privacy controls in place were overall not effective.

Security Training

We determined the DFC's overall maturity level for the Security Training program was Optimized.

DFC performed roles and responsibilities related to security training, completed a workforce assessment, and provided annual security training. Additionally, DFC addressed the knowledge, skills, and ability gaps identified through talent acquisition. DFC also measured the effectiveness of its awareness program by conducting phishing exercises and following up with additional awareness training and disciplinary action. DFC monitored and analyzed qualitative and quantitative performance measures to assess the effectiveness of its security awareness, training strategies, and plans, and received training feedback accordingly. Testing performed by the independent auditors found no exceptions for security training, and the controls were operating as intended. We determined that DFC's Security Training controls in place were overall effective.

Information Security Continuous Monitoring

We determined the DFC's overall maturity level for the ISCM program was Managed and Measurable. We identified one weakness in the ISCM domain related to the lack of assurance regarding the independence of the security assessor.

DFC Must Ensure the Assurance of the Independence of the Security Assessor

According to the NIST SP 800-53 Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*, CA-2 Control Assessment, it mandates selecting appropriate assessors, developing an assessment plan that defines scope, procedures, and roles, and obtaining approval from an authorizing official before assessment begins. The assessment must determine whether controls are correctly implemented, functioning as intended, and meeting security and privacy objectives, and then produce and distribute a formal report to the designated individuals.

A key enhancement to CA-2 is the use of independent assessors, free from conflicts of interest, to ensure objectivity and credibility in evaluating the effectiveness of controls. The authorizing official determines independence based on system risk and security category, and may include internal or external assessors, provided they are sufficiently impartial.

DFC did not document the required independence assessment for its contractor that developed DFC's security controls and performed the annual security assessment. DFC delegated the review and IT testing of security controls to a single contractor company, which was responsible for implementing controls and conducting independent testing, resulting in the contractor assessing the adequacy of their own work.

DFC management stated that the contractor has two teams working independently from each other, with one team addressing the requirements of the NIST Risk Management Framework (RMF) to prepare, categorize, select, and implement the controls, while the second team fulfills the requirements of the RMF to determine if the controls exist, are appropriate, and operating effectively. However, even if teams are organizationally separated, a conflict of interest may still exist when the same company is responsible for both implementing and assessing. As part of the RMF, DFC is required to assess the effectiveness of controls in the System Security Plan by an independent third party.

Without a proper independent assessment to determine the effectiveness of its security controls, DFC may not be able to determine the security posture of its operations and protect them. There may be a conflict of interest: the tester could be incentivized to highlight deficiencies to justify additional time and budget for improvements, or conversely, overlook control weaknesses to avoid exposing flaws in the original implementation.

We recommend that DFC's Chief Information Officer:

Recommendation 2: Assign assessors to perform tests of effectiveness on all DFC's System Security Plan with a sufficient degree of independence in accordance with National Institute of Standards and Technology Special Publication 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations, Revision 5.1.1.

Recommendation 3: Document the independence of the assessment team in the risk assessment, including organizational relationships, contract structures (if applicable), and oversight arrangements.

Recommendation 4: Ensure the risk assessment is reviewed and approved by an Authorizing Official prior to the commencement of any assessment activity.

Although DFC lacked assurance regarding the independence of the security assessor, DFC regularly analyzed performance metrics to adjust and improve its program. DFC transitioned to ongoing control and system authorization by implementing its continuous monitoring policies and strategy. In addition, DFC documented and implemented lessons learned to enhance the continuous monitoring process, instructing employees to record, analyze, and revise control activities on a cyclical basis to continuously improve DFC's security posture, as defined in the Security Continuous Monitoring Plan. Furthermore, DFC implemented its system-level continuous monitoring strategies and related processes, including conducting ongoing security control assessments, granting system authorizations, developing, and maintaining system security plans, and monitoring security controls. DFC utilized a monitoring mechanism to ensure the timely review and approval of system-level security plans.

Furthermore, DFC utilized security tools and dashboards to enhance detection accuracy and characterize threat actors, their methods, and indicators of compromise. Manual reviews were conducted for technologies that cannot be sufficiently monitored through automation. We also noted that individuals with ISCM responsibilities were held accountable by the review of DFC's performance rating template. Testing performed by the independent auditors found no exceptions for the ISCM program, and the controls were operating as intended. We determined that DFC's ISCM controls in place were overall effective.

Incident Response

We determined the DFC's overall maturity level for the Incident Response program was Managed and Measurable. However, DFC was still in the process of addressing its prior-year weakness in the incident response domain, specifically meeting the event logging (EL) level 3 requirement in accordance with OMB M-21-31.

DFC conducted tabletop exercises annually to assess the implementation of its incident response policies, and the results of these exercises indicated that the policies were effective. As a result, the DFC could be assembled quickly to meet the required reporting timelines and expedite reporting of incidents. Additionally, we noted that DFC utilized several software tools to detect suspected incidents and employed dashboards to monitor and analyze qualitative and quantitative performance measures of its incident detection and analysis policies and procedures. DFC ensured that data supporting metrics were obtained accurately, consistently, and in a reproducible format. Furthermore, DFC employed profiling techniques to establish a comprehensive baseline of network operations. RMA also noted that DFC was still in the process of meeting the event logging requirements as set forth by the OMB M-21-31 memorandum and was actively working to address these logging gaps. DFC established a [redacted] into a third-party tool through the [redacted]. Hence, we determined that FY 2024 Recommendation 1[14] remains open. Although DFC has not met the EL3 level, our overall control testing for this domain determined that the controls were operating as intended. We determined that DFC's Incident Response controls in place were overall effective.

[14] Recommendation 1 in *Fiscal Year 2024 U.S. International Development Finance Corporation Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. DFC-24-005-C, September 25, 2024).

Contingency Planning

We determined the DFC's overall maturity level for the Contingency Planning program was Managed and Measurable.

DFC's Continuity of Operations Plan was finalized, tested for effectiveness, and integrated with information contingency plans. System-level Business Impact Analyses (BIA) were integrated with enterprise risk management processes, and in conjunction with DFC's risk register. DFC consistently implemented an annual information system contingency plan testing/exercise and coordinated plan testing with external stakeholders. DFC utilized a third-party cloud software tool to track the timely review of periodic updates for BIAs and contingency tests. As such, metrics on the effectiveness of recovery activities were communicated to relevant stakeholders. Further, DFC ensured that the data supporting the metrics were obtained accurately, consistently, and in a reproducible format. Testing performed by the independent auditors found no exceptions for the Contingency Planning program, and the controls were operating as intended. We determined that DFC's Contingency Planning controls were overall effective.

Overall Conclusion

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we determined that the DFC's information security program and practices were established. They were maintained for the six Cybersecurity Framework function areas and 10 FISMA Metric Domains. We determined that the DFC's information security program and practices were effective for FY 2025, and the overall maturity level of the DFC's information security program was Managed and Measurable. Our tests of the information security program identified two findings that fell within the data protection and privacy and information security continuous monitoring domains. We made four recommendations to assist DFC in strengthening its information security program. Further, one prior FISMA performance audit recommendation remains open.

Objective, Scope, and Methodology

Objective

The objective of this performance audit was to evaluate the effectiveness of the DFC's information security program and practices and determine what maturity level the DFC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2025 IG FISMA Metrics v2.0*, dated April 3, 2025. Specifically, the performance audit determined whether DFC implemented an effective information security program by evaluating the six Cybersecurity Framework function areas as divided into 10 FISMA Metric Domains:

- **Govern**, includes metrics pertaining to cybersecurity governance and cybersecurity supply chain risk management;
- **Identify**, includes metrics pertaining to risk and asset management;
- **Protect**, includes metrics pertaining to configuration management, identity and access management, data protection and privacy, and security training;
- **Detect**, includes metrics pertaining to information security continuous monitoring;
- **Respond**, includes metrics pertaining to incident response; and
- **Recover**, includes metrics pertaining to contingency planning.

Scope

We conducted this performance audit 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 performance audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objectives.

The scope of the FISMA performance audit work was agency-wide for the DFC, and the review covered FY 2025 as of August 1, 2025. We assessed all four FISMA reportable systems from the DFC's inventory of information systems. The performance audit fieldwork covered DFC's headquarters in Washington, DC, and audit work was conducted between February 3 and August 1, 2025. This performance audit included steps to follow up on deficiencies from the prior year. Appendix I: Status of Prior Year Findings provides a summary of the status of recommendations from the prior year.

Methodology

The overall strategy of our performance audit considered the following: (1) NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*; (2) NIST SP 800-53A, Revision 5.1.1 *Assessing Security and Privacy Controls in Information Systems and Organizations*; (3) *FY 2025 IG FISMA Reporting Metrics v2.0*; and (4) the DFC's policies and procedures.

We conducted interviews with DFC officials and reviewed the legal and regulatory requirements stipulated in FISMA. We also examined documents supporting the information security program and practices. Where appropriate, we compared documents, such as the DFC's information technology policies and procedures, to requirements stipulated in NIST Special Publications. Additionally, we conducted tests of system processes to assess the design and operating effectiveness of these controls.

In testing the effectiveness of the security controls relevant to the 20 core metric questions and 5 FY 2025 supplemental metric questions specified in OMB's *FY 2025 IG FISMA Metrics v2.0*, dated April 3, 2025, we tested the entire DFC administrative controls population. The application controls were the responsibility of DFC's service providers.

We applied the following criteria for performing the DFC's FY 2025 FISMA audit:

NIST Federal Information Processing Standards (FIPS) and SPs

- *NIST Cybersecurity Framework (CSF 2.0)*
- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5.1.1, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*
- NIST SP 800-63-3, *Digital Identity Guidelines*

- NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*
- NIST SP 800-207, *Zero Trust Architecture*
- NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1, Recommendations for Mitigating the Risk of Software Vulnerabilities*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments: Volume 1: Overview*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OMB Policy Directives

- *FY 2025 IG FISMA Reporting Metrics v2.0*
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*
- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*

- OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Memorandum M-17-09, *Management of Federal High Value Assets*
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CISP) for the Federal Civilian Government*
- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

Government Accountability Office

- Standards for Internal Control in the Federal Government, September 2014

Cybersecurity and Infrastructure Security Agency

- Binding Operational Directive (BOD) 25-01, *Implementing Secure Practices for Cloud Services*
- BOD 23-02, *Mitigating the Risk from Internet-Exposed Management Interfaces*
- BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*
- BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- BOD 18-02, *Securing High Value Assets*
- BOD 18-01, *Enhance Email and Web Security*
- BOD 17-01, *Removal of Kaspersky-Branded Products*
- BOD 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- BOD 16-02, *Threat to Network Infrastructure Devices*
- Emergency Directive (ED) 24-02*, Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*
- ED 24-01 *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*
- ED 22-03 *Mitigate VMware Vulnerabilities*
- ED 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- ED 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*
- ED 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*
- ED 21-01, *Mitigate SolarWinds Orion Code Compromise*
- ED 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*
- ED 20-03, *Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 2020 Patch Tuesday*
- ED 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- ED 19-01, *Mitigate DNS Infrastructure Tampering*

Appendix I: Status of Prior Year Recommendations

The following table provides the status of the FY 2024 FISMA performance audit recommendations.

Table 3: FY 2024 FISMA Performance Audit Report A-DFC-25-005-C Recommendations

Recommendation No.	Audit Recommendations	DFC's Position	Auditor's Position on the Status
1	We recommend that DFC's Chief Information Officer fully implement event logging requirements in accordance with the Office of Management and Budget, Memorandum M-21-31.	Open	Agree. Refer to Audit Results – Incident Respond domain

Appendix II: Management Response

MEMORANDUM September 8, 2025

TO: Erika Ersland
Acting Assistant Inspector General for Audits DFC – Office of the Inspector General (OIG)

FROM: Willie Williams
Acting Vice President and Chief Information Officer

WILLIE WILLIAMS Digitally signed by WILLIE WILLIAMS
Date: 2025.09.08 14:05:07 -04'00'

SUBJECT: Fiscal Year 2025 DFC Federal Information Security Modernization Act of 2014 Audit Response

The U.S. International Development Finance Corporation (DFC) management appreciates the comprehensive report produced by the Office of the Inspector General (OIG). We are pleased that the audit recognized the Corporation's effectiveness, resulting in an overall information security program maturity rating of "Level 4 – Managed and Measurable."

The draft report contained four recommendations, which we address in detail below:

<u>Recommendation 1</u>: Periodically perform a physical inventory of all mobile devices, including those pending disposal, to ensure all assets are accounted for and accurately reflected in the asset tracking system.

Management Response: DFC concurs with the recommendation. DFC has already implemented robust improvements to its mobile device management program to ensure full traceability and accountability, including:

- All DFC-issued mobile devices are now enrolled in our device management platforms.
- Devices enforce encryption, passcode policies, activation lock, and remote wipe capabilities.
- Devices are physically tagged and tracked in ServiceNow.
- Weekly physical inventory checks are conducted.
- Comprehensive review and reconciliation processes have been established for devices pending disposal.
- Secure disposal procedures have been established for devices that cannot be powered on.

Estimated Completion Date: Immediate (Already Implemented)

<u>Recommendation 2</u>: Assign assessors to perform tests of effectiveness on all DFC's System Security Plan with a sufficient degree of independence in accordance with NIST Special Publication 800-53A.

Management Response: DFC concurs with the recommendation. DFC has completed corrective actions to ensure appropriate independence for all security control assessors. We have formalized a process that assigns Security Control Assessors (SCAs) who are organizationally and contractually independent from the development, implementation, and operation of the systems they assess**.** This separation prevents conflicts of interest and ensures that assessors can provide an unbiased evaluation of control effectiveness, in alignment with NIST SP 800-53A requirements.

Estimated Completion Date: Immediate (Already Implemented)

Recommendation 3: Document the independence of the assessment team in the risk assessment, including organizational relationships, contract structures, and oversight arrangements.

Management Response: DFC concurs with the recommendation. DFC has completed corrective actions by implementing a formal process to document the independence of the assessment team. A formal memorandum is now used to officially document assessor independence and specifically outlines the organizational and contractual relationships of assessors, the separation of duties and reporting lines, and the mechanisms for oversight and quality assurance. The Chief Information Security Officer (CISO) is responsible for the oversight of all assessment activities and ensures this documentation is included in the Security Assessment Plan (SAP) and Security Assessment Report (SAR) for each system.

Estimated Completion Date: Immediate (Already Implemented)

Recommendation 4: Ensure the risk assessment is reviewed and approved by an Authorizing Official prior to the commencement of any assessment activity.

Management Response: DFC concurs with the recommendation. DFC has completed corrective actions by implementing a procedure requiring the submission of a formal memorandum and supporting documentation to the Authorizing Official for review and approval. This ensures transparency and provides the Authorizing Official with full visibility into the independence of the assessment team, supporting DFC's compliance with federal requirements for objective security control assessments. This approval is maintained as part of the system's official assessment and authorization package and records

Estimated Completion Date: Immediate (Already Implemented)

/s/

Appendix III: Evaluation of Management Response

In response to the draft report, DFC's comments are included in Appendix II: Management Response. Management indicated that corrective actions were already implemented immediately to address Fiscal Year (FY) 2025 - Recommendations 1, 2, 3, and 4.

Based on our evaluation of management comments, we acknowledge DFC's management decisions on the new recommendations and believe the actions taken and planned will resolve the issues identified in the report.

Appendix IV: Glossary of Acronyms

BIA	Business Impact Analysis
BOD	Binding Operational Directive
CIGIE	Council of the Inspectors General on Integrity and Efficiency
C-SCRM	Cybersecurity Supply Chain Risk Management
CSF	Cybersecurity Framework
DFC	U.S. International Development Finance Corporation
DHS	Department of Homeland Security
DNS	Domain Name System
ED	Emergency Directive
EL	Event Logging
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RMA	RMA Associates, LLC
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SP	Special Publication
ZTA	Zero Trust Architecture