OFFICE OF INSPECTOR GENERAL

U.S. International Development Finance Corporation

DFC's Fiscal Year 2026 Federal Information Security Modernization Act of 2014 Performance Audit

September 30, 2026
Audit Report DFC-26-005-C

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

Report Highlights

Office of Inspector General
International Development Finance Corporation

DFC's Fiscal Year 2026 Federal Information Security Modernization Act of 2014 Performance Audit

What Was Reviewed

The United States International Development Finance Corporation's (DFC) Office of Inspector General (OIG) contracted with the independent public accounting firm RMA Associates, LLC (RMA) to conduct the Fiscal Year (FY) 2026 Federal Information Security Modernization Act of 2014 (FISMA) performance audit of DFC.

The audit's objective was to evaluate the effectiveness of DFC's information security program and practices and determine DFC's maturity level for each of the core and supplemental metrics outlined in the FY 2025 Inspectors General (IG) FISMA Reporting Metrics v2.0 (April 2025). For the FY 2026 audit cycle, Inspectors General and independent external auditors used FY 2025 IG FISMA reporting metrics and associated implementation guidance.

What Was Found

RMA determined that DFC's information security program and practices were effective for FY 2026. DFC's information security program met the criteria required to achieve a maturity level of Managed and Measurable, considered effective under the IG FISMA reporting metrics. RMA's testing of DFC's information security program identified four findings affecting risk and asset management, data protection and privacy, information security continuous monitoring, and contingency planning domains.

Recommendations

RMA made eight recommendations to DFC's Chief Information Officer and Chief Operating Officer to address four findings and further strengthen DFC's information security program. Specifically, RMA recommended that DFC's Chief Information Officer:

- **Recommendation 1**: Update the Asset Management Policy and Procedures and implement procedures for timely tracking of all assets, including those pending return, in storage, or for disposal.
- **Recommendation 2**: Review and dispose of long-term stored assets and ensure all devices are securely wiped prior to disposal.
- **Recommendation 3**: Establish thresholds and escalation procedures for aging inventory.

- **Recommendation 4**: Implement validation controls to ensure accurate recording of asset details (e.g., type, model, serial number, asset tag).
- **Recommendation 5**: Restrict and monitor updates to asset records and enforce dual authorization for implementing significant status changes (e.g., disposal, availability).
- **Recommendation 6**: Ensure all hardware, including hardware that does not contain data, is consistently tagged with unique identifiers.
- **Recommendation 7**: Perform a comprehensive physical inventory count and reconcile all hardware assets with the third-party service provider inventory system.

Additionally, RMA recommended that DFC's Chief Operating Officer:

- **Recommendation 8**: Implement a centralized tracking mechanism (e.g., compliance tracker, Governance, Risk, and Compliance tool, or calendar-based system) to monitor key milestones, due dates, and approvals of the COOP.

MEMORANDUM

Date: September 30, 2026

To: Mr. Willie Williams
Vice President and Chief Information Officer

From: Ms. Erika Ersland
Acting Supervisor Auditor

Subject: DFC's Fiscal Year 2026 Federal Information Security Modernization Act of 2014 Performance Audit (Report Number DFC-26-005-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 2026 to evaluate the effectiveness of DFC's information security program and practices and determine what maturity level DFC achieved for each core and supplemental metric 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's (OMB) *FY 2025 IG FISMA Reporting Metrics v2.0*, OMB Circular No. A-130, Section 522 of the Consolidated Appropriations Act of 2005, and others, such as National Institute of Standards and Technology (NIST) standards.

In this performance audit of DFC, RMA reported the information security program and practices were effective in FY 2026, as DFC's information security program met the criteria required to achieve a maturity level of Managed and Measurable (Effective). RMA's tests the information security program identified four findings affecting risk and asset management, data protection and privacy, information security continuous monitoring, and contingency planning domains.

RMA is responsible for the attached auditor's report dated September 23, 2026, and the conclusions expressed therein. We do not express opinions on DFC's information systems, 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: Chief Financial Officer
Chief Operating Officer
Chief Information Security Officer
Deputy General Counsel
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 2026

Sensitive but Unclassified – this report includes sensitive information regarding DFC information systems and cannot be shared without OIG's express permission.

RMA | Associates
Auditors. Consultants. Advisors.

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

September 23, 2026

Dan Loveland
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* Performance Audit Report for Fiscal Year 2026

Dear Mr. Loveland:

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) 2026. In accordance with the *Federal Information Security Modernization Act of 2014* (FISMA), the objective of this performance audit was to evaluate the effectiveness of DFC's information security program and practices and determine the maturity level achieved for each core and supplemental metric. For the FY 2026 audit cycle, Inspectors General and independent external auditors continued to use the *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, and associated implementation guidance. The performance audit fieldwork covered DFC's headquarters in Washington, DC, from February 19, 2026, to July 31, 2026.

Based on our performance audit results, we determined that DFC's information security program and practices were effective for FY 2026, as the criteria assessed for DFC's information security program met the maturity level of Managed and Measurable, considered effective under the IG FISMA reporting metrics. Our assessment of the information security program identified four findings that fell within the risk and asset management, data protection and privacy, information security continuous monitoring, and contingency planning domains. We made eight recommendations to assist DFC in strengthening its information security program. Further, DFC closed three of five recommendations from the prior-year FISMA audits.

Our report includes **Appendices I**: Status of Prior-Year Recommendations, **II**: Management's Response, **III**: Evaluation of Management's Responses, and **IV**: Glossary of Acronyms.

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.

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

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

and Budget (OMB). We considered the guidelines established by 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 2026, OMB required Inspectors General to assess 25 metrics from *FY 2025 IG FISMA Reporting Metrics v2.0*, 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 and 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* classifies information security programs and practices into five maturity levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

We also prepared responses to OMB's M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, which encourages agencies to shift towards a continuous assessment process for their annual independent assessment using *FY2025 IG FISMA Reporting Metrics v2.0*, 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 July 31, 2026. We have no obligation to update our report or to revise the information contained therein to reflect events occurring after July 31, 2026.

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

Sincerely,

RMA Associates

RMA Associates, LLC
Arlington, VA

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

Table of Contents

Introduction 1

Background 1

United States International Development Finance Corporation 1

Federal Information Security Modernization Act of 2014 2

Key Changes to the FY 2026 IG FISMA Reporting Metrics 3

FY 2025 Change That Continues to Apply in FY 2026 3

Summary Performance Audit Results 4

Objective, Scope, and Methodology 15

Appendix I: Status of Prior-Year Recommendations 22

Appendix II: Management's Response 23

Appendix III: Evaluation of Management's Response 27

Appendix IV: Glossary of Acronyms 28

RMA Associates
Auditors. Consultants. Advisors.

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

Introduction

This report presents the results of RMA Associates, LLC (RMA)'s independent performance audit of the United States International Development Finance Corporation's (DFC) information security program and practices. The *Federal Information Security Modernization Act of 2014* (FISMA) requires federal agencies to conduct an annual independent audit to assess their information security program and practices, determine the effectiveness of such programs and practices, and report the results of the audit 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 core and supplemental metric outlined in the *Fiscal Year (FY) 2025 Inspectors General (IG) FISMA Reporting Metrics v2.0*, dated April 2025.

As part of our performance audit, we audited DFC according to 20 core and five supplemental metrics specified in OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*.[1] These metrics provide reporting requirements across function areas to be addressed in the independent assessment of agencies' information security programs.[2] We also considered applicable DFC and OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards.

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). Congress renewed DFC authorities for six years, through December 2031, in the DFC Modernization and Reauthorization Act of 2025. 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.

The U.S. International Development Finance Corporation (DFC) is the international investment arm of the United States Government and central to U.S. economic statecraft. DFC's mission is to mobilize private capital to advance U.S. foreign policy and economic development. DFC's investments are to deliver strong returns for American taxpayers, drive meaningful economic development for U.S. allies and partners, and secure supply chains to counter and outcompete

[1] 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.
[2] Refer to section titled, *Objective, Scope, and Methodology,* for more details.

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

adversaries. DFC invests across energy, critical minerals, infrastructure, information and communication technology, healthcare, and agribusiness sectors.

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 secure 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 modernized 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 agency compliance and reporting that is more concentrated on 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. 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 security controls planned or in place to protect 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.[3]

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,

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

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

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.[4] FISMA authorized the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.[5]

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 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.[6]

Key Changes to the FY 2026 IG FISMA Reporting Metrics

For FY 2026, IG's and independent external auditors were directed to use the *FY 2025 IG FISMA Reporting Metrics v2.0* and associated implementation guidance. Accordingly, the FY 2026 audit did not introduce a new set of IG FISMA reporting metrics.

FY 2025 Change That Continues to Apply in FY 2026

One of the goals of the annual FISMA audits is to assess agencies' progress toward achieving objectives that strengthen federal cybersecurity. The *FY 2025 IG FISMA Reporting Metrics v2.0* were 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.

[4] Ibid.
[5] Ibid.
[6] Ibid.

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

To align with CSF 2.0, the supply chain risk management (SCRM) domain was moved from the Identify function area to the Govern function area and renamed 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.

- 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.

Summary Performance Audit Results

We determined that, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards, DFC's information security program and practices were established and maintained for the six NIST Cybersecurity Framework functions[7] and 10 FISMA Metric Domains.[8] The overall maturity level of DFC's information security program was Managed and Measurable as described in this report. Accordingly, we determined DFC's information security program and practices were effective for FY 2026.

We provided 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 in subsequent correspondence provided target completion dates for recommendations (refer to **Appendix II**: Management's Response for DFC's response in its entirety and **Appendix III**: Evaluation of Management's Response for our assessment of management's response).

During FY 2026, DFC closed three of five recommendations from the FY 2024 and FY 2025 FISMA audits. **Appendix I**: Status of Prior-Year Recommendations summarizes the status of recommendations from prior years.

[7] 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 *CSF 2.0*.
[8] 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.

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

The maturity level for the 10 domains is presented in **Table 1: DFC's FY 2026 Maturity Levels**.

Table 1: DFC's FY 2026 Maturity Levels

Function	Maturity Level	
Function 1: Govern		Managed and Measurable (Level 4)
• Cybersecurity Governance	Managed and Measurable (Level 4)	
• Cybersecurity Supply Chain Risk Management	Optimized (Level 5)	
Function 2: Identify – Risk and Asset Management		Managed and Measurable (Level 4)
Function 3: Protect		Managed and Measurable (Level 4)
• Configuration Management	Managed and Measurable (Level 4)	
• Identity and Access Management	Optimized (Level 5)	
• Data Protection and Privacy	Consistently Implemented (Level 3)	
• Security Training	Optimized (Level 5)	
Function 4: Detect – Information Security Continuous Monitoring		Consistently Implemented (Level 3)
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**

Our testing identified weaknesses affecting the Risk and Asset Management, Data Protection and Privacy, Information Security Continuous Monitoring, and Contingency Planning domains. Data Protection and Privacy and Information Security Continuous Monitoring were assessed at the Consistently Implemented maturity level, while the remaining domains were assessed at Managed and Measurable or Optimized. Based on the results of the core metrics, supplemental metric data points, and our risk-based assessment of the six Cybersecurity Framework function areas, DFC achieved an overall maturity level of Managed and Measurable. Accordingly, we determined that DFC's information security program and practices were effective for FY 2026.

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

Cybersecurity Governance

We determined DFC's overall maturity level for the Cybersecurity Governance domain was Managed and Measurable.

Our testing found that DFC had finalized and authorized its current and target cybersecurity profiles in alignment with CSF 2.0. DFC assessed gaps between its current and target profiles and implemented a prioritized action plan. In addition, profiles were reviewed annually to align with DFC's risk strategy. Also, 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

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

responsibilities effectively. Our testing found no exceptions for the Cybersecurity Governance domain, and the controls were operating as intended. We determined that DFC's Cybersecurity Governance controls were overall effective.

Cybersecurity Supply Chain Risk Management

We determined DFC's overall maturity level for the C-SCRM domain 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. Our testing found no exceptions for the C-SCRM domain, and the controls were operating as intended. We determined that DFC's C-SCRM controls were overall effective.

Risk and Asset Management

We determined DFC's overall maturity level for the Risk and Asset Management domain was Managed and Measurable. We identified one weakness in the Risk and Asset Management domain related to hardware asset management.

Hardware Asset Management

We conducted a site visit to DFC Headquarters to observe how DFC tracks and maintains its hardware asset inventory. During the site visit, DFC Management informed RMA that certain assets located in the storage room were not included in the inventory system and therefore were not part of the inventory population available for selection. The following items in the storage room were not recorded:

- 15 devices, which were pending return to the vendor;
- Approximately 800 devices, which had been stored for an extended period; and
- Multiple devices, which were considered low-risk by DFC Management.

RMA noted that 4,783 devices were listed as "Unassigned" and "Surplus" in the inventory records.

RMA assessed completeness by selecting a judgmental sample of 10 items observed on site in the storage room and traced them back to the inventory record. We found that two out of 10 sampled items from storage were not accurately recorded in the third-party service provider inventory system.

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

RMA verified existence by selecting a judgmental sample of 10 items from a population of 8,956 inventory items in the master inventory spreadsheet. We found that nine out of 10 sampled items had exceptions noted, meaning deviations between the master inventory spreadsheet and the hardware found in the storage room.

DFC Office of Information Technology (OIT) Asset Management Policy requires quarterly record reconciliations and an annual wall-to-wall inventory to account for all assets in the Configuration Management Database and during manual inventory. In addition, NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* CM-5 Access Restrictions For Change requires organizations to control and approve system changes, limit and periodically review production privileges, and maintain accurate system component inventories. CM-8 System Component Inventory requires organizations to create and maintain a detailed inventory of all system components, including 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.

DFC OIT's Asset Management Procedures and control activities were not effectively implemented to ensure that hardware inventory and disposal actions were accurately reflected in the asset management system and that hardware assets were appropriately accounted for throughout their lifecycle. In addition, DFC lacked adequate governance and approval controls over third-party service provider inventory system and did not perform sufficient periodic reconciliations between physical inventory and system records, as required by DFC's Asset Management Policy. DFC Management stated that DFC was currently enforcing asset-tagging requirements and, due to limited staffing, DFC tracked only devices that contained data based on risk considerations.

Untracked and unverified devices may expose DFC to data security breaches because equipment stored for extended periods without being wiped may retain sensitive information vulnerable to unauthorized access. Without appropriately tracking hardware devices, the risk of asset loss, theft, or misappropriation also increases. Inaccurate and incomplete inventory records also reduce the reliability of the third-party service provider's inventory system, leading to misinformed decisions, inefficient asset use, and unnecessary procurement costs.

We recommend that the DFC Chief of Information Office:

Recommendation 1: Update the Asset Management Policy and Procedures and implement procedures for timely tracking of all assets, including those pending return, in storage, or for disposal.

Recommendation 2: Review and dispose of long-term stored assets and ensure all devices are securely wiped prior to disposal.

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

Recommendation 3: Establish thresholds and escalation procedures for aging inventory.

Recommendation 4: Implement validation controls to ensure accurate recording of asset details (e.g., type, model, serial number, asset tag).

Recommendation 5: Restrict and monitor updates to asset records and enforce dual authorization for implementing significant status changes (e.g., disposal, availability).

Recommendation 6: Ensure all hardware, including hardware that does not contain data, is consistently tagged with unique identifiers.

Recommendation 7: Perform a comprehensive physical inventory count and reconcile all hardware assets with the third-party service provider inventory system.

Overall Risk and Asset Management Assessment

DFC maintained comprehensive and accurate inventories of its information systems and software assets and used automated systems to monitor the lifecycle of software assets. DFC also maintained an inventory of its data and corresponding metadata for each data type and subjected those inventories to the monitoring processes defined in its information security continuous monitoring strategy.

Although our testing identified the hardware asset management weaknesses described above, these weaknesses did not reduce the overall Risk and Asset Management domain below the Managed and Measurable maturity level. The remaining Risk and Asset Management controls tested were operating as intended, and DFC met the applicable maturity criteria for its risk management, information system inventory, software asset management, and data management activities. Based on results of the core and supplemental metrics and our risk-based assessment, we determined that DFC's Risk and Asset Management domain achieved a maturity level of Managed and Measurable and was overall effective. However, DFC's hardware asset management controls were not operating effectively.

Configuration Management

We determined DFC's overall maturity level for the Configuration Management domain 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. DFC managed its vulnerabilities by using Security Content Automation Protocol-validated software scanning tools on all systems and providing scan reports. In addition, DFC used various automated mechanisms to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit

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

any security impact and mitigate the spike in vulnerabilities. Although outstanding vulnerabilities were found during 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. Applicable patches or remediation actions were automatically applied when the laptops were powered on and reconnected to the network. Our testing identified no exceptions in the Configuration Management domain, and the controls tested were operating as intended. Accordingly, we determined that DFC's Configuration Management controls were overall effective.

Identity and Access Management

We determined DFC's overall maturity level for the Identity and Access Management domain 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. DFC's systems interface with the solution to oversee employees, resulting in the ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness in near real time. DFC's implementation of its single sign-on solution and integration with Active Directory demonstrated that DFC employed automated mechanisms to manage privileged accounts, including the automatic removal of temporary, emergency, and inactive accounts.

Additionally, DFC used lessons learned; end users' devices were properly configured, and privileged users used a strong authentication mechanism. Our testing found no exceptions for the Identity and Access Management domain, and the controls were operating as intended. We determined that DFC's Identity and Access Management controls were overall effective.

Data Protection and Privacy

We determined DFC's overall maturity level for the Data Protection and Privacy domain was Consistently Implemented. We identified one weakness[9] in the Data Protection and Privacy domain related to the lack of adequate accountability over hardware asset inventory, including mobile devices.

Hardware Accountability and Sanitization

[9] Please refer to Risk and Asset Management section for details.

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

During the site visit to DFC Headquarters, we found that:

- Approximately 800 devices, which had been stored for an extended period of time, had not been sanitized and were awaiting management approval for disposal.

In addition, our existence testing could not locate five of 10 devices. Therefore, we could not confirm whether hardware was tracked and sanitized adequately.

Because DFC could not locate the devices, RMA could not verify whether the devices remained under DFC control or whether applicable sanitization requirements had been completed.

According to NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* MP-6 Media Sanitization requires organizations to sanitize system media before disposal, release, or reuse using approved techniques, with sanitization mechanisms appropriate to the information's security category or classification. It also requires organizations to review, approve, track, document, and verify media sanitization and disposal actions.

DFC OIT's Asset Management Policy and Procedures were not suitably designed to ensure OIT hardware inventory and disposal actions were accurately reflected in the OIT asset management inventory system, and ensured media were properly sanitized and disposal actions performed. DFC must sanitize hardware before disposal; however, the high volume of devices and limited resources delayed this process.

Untracked or untagged devices may still contain sensitive data. If lost or stolen, this data could be compromised, especially if the devices are not properly sanitized or encrypted. Additionally, if a hardware asset 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 are taken.

As such, RMA determined that FY 2025 Recommendation 1[10] remains open and did not make a new recommendation for the Data Protection and Privacy domain.

Notwithstanding the hardware sanitization and accountability weakness described above, DFC implemented several mature data protection and privacy practices, including monitoring quantitative and qualitative performance measures, conducting an independent review of its privacy program, maintaining data exfiltration capabilities, and incorporating lessons learned from privacy breach exercises.

However, DFC could not demonstrate complete accountability for certain hardware devices that may contain sensitive information or provide assurance regarding their disposition and sanitization status. This unresolved weakness prevented DFC from satisfying the Managed and Measurable

[10] Recommendation 1 in *Fiscal Year 2025 U.S. International Development Finance Corporation Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. DFC-25-005-C, October 9, 2025).

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

criteria for the applicable Data Protection and Privacy metric question. Accordingly, we determined that DFC's Data Protection and Privacy domain remained at the Consistently Implemented maturity level and was not effective.

Security Training

We determined DFC's overall maturity level for the Security Training domain 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, reorganization, and reassigned responsibilities. 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. Our testing found no exceptions for the Security Training domain, and the controls were operating as intended. We determined that DFC's Security Training controls were overall effective.

Information Security Continuous Monitoring

We determined DFC's overall maturity level for the Information Security Continuous Monitoring (ISCM) domain was Consistently Implemented. We identified one weakness in the ISCM domain related to inconsistency between Cybersecurity Policies and the ISCM Plan.

Inconsistency between Cybersecurity Policies and Information Security Continuous Monitoring Plan

We examined 36 cybersecurity policies and procedures and found 12 instances where the defined review cycles in the policies were different from the ISCM Plan. Specifically, Cybersecurity Policies require annual review for security policies, while the ISCM Plan requires a biennial or as-needed review.

According to NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, PL-1 Policies and Procedures, organizations are required to develop, document, and disseminate planning policies consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

DFC Management stated that they had recently changed the practice from an annual review to a biennial review. The inconsistency resulted from a lack of centralized governance and coordination during the update of cybersecurity policies and the ISCM Plan, leading to independently defined review cycles.

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

The misalignment created ambiguity in governance expectations. Inconsistent review cycles may result in cybersecurity policies and procedures not being reviewed and updated within appropriate or consistent timeframes. As a result, policies may become outdated, leading to potential misalignment with current security requirements, standards, and organizational practices.

During fieldwork, DFC Management promptly implemented corrective actions by updating and approving 19 cybersecurity policies and procedures. These updates align with the ISCM plan by establishing a biennial review cycle for cybersecurity policies. Accordingly, RMA has no further recommendations for this finding and considers it closed.

We also noted that DFC used security tools and dashboards to enhance detection accuracy and characterize threat actors, their methods, and indicators of compromise. Individuals with ISCM responsibilities were held accountable by the review of DFC's performance rating. Additionally, 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. 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 used a monitoring mechanism to ensure the timely review and approval of system-level security plans. DFC engaged with an independent external security control assessment firm to conduct security control effectiveness testing of DFC systems. Independence of the assessment team was documented in the risk assessment, and the risk assessment was reviewed and approved by an Authorizing Official prior to the commencement of an assessment activity. As a result, we determined that FY 2025 Recommendations 2, 3, and 4[11] are now closed. Although our testing found one exception for the ISCM domain, DFC promptly took corrective actions, and controls were operating as intended. We determined that DFC's ISCM controls were overall effective.

Incident Response

We determined DFC's overall maturity level for the Incident Response domain was Managed and Measurable. However, DFC was still in the process of addressing its prior-year weakness in this domain, specifically meeting the event logging level 3 requirement in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.

[11] Recommendations 2, 3, and 4 in *Fiscal Year 2025 U.S. International Development Finance Corporation Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. DFC-25-005-C, October 9, 2025).

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

DFC used 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 event logging requirements as set forth by OMB M-21-31 memorandum and was actively working to address these gaps. On May 22, 2026, OMB issued Memorandum M-26-14, *Ensuring Effective and Efficient Logging and Network Visibility to Defend Against Evolving Cyber Threats*, which rescinded M-21-31. M-26-14 requires the Cybersecurity and Infrastructure Security Agency to publish a Logging Reference Architecture within 90 days (i.e., by August 20, 2026). Agencies must then develop logging plans within 90 days of that release (i.e., November 18, 2026), addressing continuous event monitoring, threat hunting, investigation, response, and forensics based on their threat environment, risk profile, and mission. Therefore, agencies are not required to complete logging plans or begin implementation until FY 2027, after the FY 2026 IG FISMA reporting cycle. We determined that FY 2024 Recommendation 1[12] remains open until DFC demonstrates compliance with M-26-14. Although DFC did not meet the event logging level 3, our overall control testing for the Incident Response domain determined that the controls were operating as intended. We determined that DFC's Incident Response controls were overall effective.

Contingency Planning

We determined DFC's overall maturity level for the Contingency Planning domain was Managed and Measurable. We identified one weakness in the Contingency Planning domain related to an outdated Continuity of Operations Plan (COOP).

Outdated Continuity of Operations Plan

DFC did not perform the required annual update of the COOP. The latest approved version on record dates to 2024. DFC's COOP was not updated, tested for effectiveness, and integrated with information contingency plans.

According to DFC's COOP, mission essential functions and supporting activities must be reviewed and updated annually by the Continuity Coordinator as part of the maintenance process, with the COOP Manager responsible for the review and update. *Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements* also requires continuity programs to address all continuity elements and phases, maintain an approved continuity plan, and document annual reviews and updates.

DFC's organizational changes resulted in unclear roles and responsibilities, leading to gaps in governance and oversight for the COOP. In addition, DFC did not establish a formalized

[12] 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).

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

monitoring and control framework, such as assigned ownership and a tracking process to ensure the timely review, update, and approval of the COOP.

Without consistently reviewing and authorizing the COOP, DFC may be unable to ensure that it can continue performing essential functions during a wide range of emergencies.

During fieldwork, DFC Management promptly implemented corrective action by documenting a memorandum to establish ownership and accountability for its COOP. DFC assigned two individuals to serve as the COOP Coordinator and COOP Program Manager, with responsibility for overseeing the annual review, update, testing, and approval process.

We recommend that the DFC Office of the Chief Operating Officer:

Recommendation 8: Implement a centralized tracking mechanism (e.g., compliance tracker, Governance, Risk, and Compliance tool, or calendar-based system) to monitor key milestones, due dates, and approvals of the COOP.

Overall Contingency Planning Assessment

RMA also noted that 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 used a third-party cloud software tool to track timely reviews 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. Although our testing found one exception for the Contingency Planning domain, 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 DFC's information security program and practices were established and maintained across the six Cybersecurity Framework function areas and 10 FISMA Metric Domains. As such, DFC's information security program and practices were effective for FY 2026, and the overall maturity level was Managed and Measurable. Our tests of the information security program identified four findings that fell within the risk and asset management, data protection and privacy, information security continuous monitoring, and contingency planning domains. We made eight recommendations to assist DFC in strengthening its information security program. Further, DFC closed three of five recommendations from the prior-year FISMA audits.

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

Objective, Scope, and Methodology

Objective

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

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

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 objective. 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, and the review covered FY 2026 as of July 31, 2026. We assessed all four FISMA reportable systems from DFC's inventory of information systems. The performance audit fieldwork covered DFC's headquarters in Washington, DC, and audit work was conducted between February 19 and July 31, 2026. This performance audit included steps to follow up on deficiencies from the prior years. **Appendix I**: Status of Prior-Year Recommendations summarizes the status of recommendations from the prior years.

Methodology

The overall strategy of our performance audit considered the following: (1) NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*; (2) NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and*

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

Organizations; (3) *FY 2025 IG FISMA Reporting Metrics v2.0*; and (4) DFC's policies and procedures. Our testing procedures were developed from NIST SP 800-53A, Revision 5.

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 DFC documents, such as their information technology policies and procedures, to requirements stipulated in NIST SPs. 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 and five supplemental metric questions specified in OMB's *FY 2025 IG FISMA Reporting 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.

OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, directed IGs to report the assessed maturity levels of these metrics in CyberScope.[13] These metrics were aligned with the six function areas in the *NIST CSF 2.0* as follows:

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

For each of the 20 core and five supplemental metric questions in the *FY 2025 IG FISMA Reporting Metrics v2.0*, we assessed DFC's implementation against the applicable maturity-level criteria. Each criterion was evaluated to determine whether it had been satisfied. Those results formed the basis of DFC's maturity level for each metric. The core and supplemental metrics were averaged separately to determine each domain's overall maturity level and assess the effectiveness of DFC's information security program and functions.

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 classify information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and

[13] 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.

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

Optimized. Within the context of the maturity model, Level 4 (Managed and Measurable) and Level 5 (Optimized) represent an effective level of security. **Table 2: IG Audit Maturity Levels** explains the five maturity model levels.

Table 2: 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 2026, IGs used the *FY 2025 IG FISMA Reporting Metrics v2.0* and 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 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 four function areas is Level 4 (Managed and Measurable), then the information security program rating would average a 3.60.[14]

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 computed average of the maturity level was 4.10, Managed and Measurable. As a result, DFC's overall assessed maturity level was effective.

DFC's FY 2026 calculated core metric, supplemental metric, assessed maturity averages, and assessed maturity level by function are presented in **Table 3: Overall Calculated Averages Maturity Calculation in FY 2026**.

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

Sensitive but Unclassified – this report includes sensitive information regarding DFC information systems and cannot be shared without OIG's express permission.

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

Table 3: Overall Calculated Averages Maturity Calculation in FY 2026

Function	Core Metrics	Supplemental Metrics	Assessed Maturity Average	Assessed Maturity
Govern[15]	5.00	4.33	4.43	Managed and Measurable
Identify	4.00	4.00	4.00	Managed and Measurable
Protect	4.50	N/A	4.50	Managed and Measurable
Detect	3.50	4.00	3.67	Consistently Implemented
Respond	4.00	N/A	4.00	Managed and Measurable
Recover	3.50	N/A	4.00	Managed and Measurable
Overall Maturity	**4.08**	**4.11**	**4.10**	**Managed and Measurable**

For FY 2026, 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.

Since FY 2025, OMB and CIGIE piloted a weighted-average approach to IG FISMA scoring that gives greater importance to certain foundational cybersecurity metrics and accounts for dependencies between them. The goal was to better reflect cybersecurity effectiveness, recognizing that areas such as Cybersecurity Governance and Risk and Asset Management support the successful implementation of activities like continuous monitoring, configuration compliance, and ongoing authorizations. The weighted scoring was calculated automatically through CyberScope. According to *FY 2025 IG FISMA Reporting Metrics v2.0,* foundational metrics are metrics 1, 2, 3, 7, 8, 9, 10, and 33. The weighted average approach will be ((FY 2025 Foundational Metric Maturity x 2) + (FY 2025 Remaining Core x 1))/3.[16]

Criteria

We applied the following criteria for performing DFC's FY 2026 FISMA audit:

NIST Federal Information Processing Standards (FIPS) and SPs

- *NIST 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*

[15] The Govern function area was introduced in FY 2025.
[16] *FY 2025 IG FISMA Reporting Metrics v2.0*, April 3, 2025.

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

- 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, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5, *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 800-63-4, *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 800-115, *Technical Guide to Information Security Testing and Assessment*
- 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)*

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

OMB Policy Directives

- *FY 2025 IG FISMA Reporting Metrics v2.0*
- OMB Memorandum M-26-14, *Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats*
- OMB Memorandum M-26-05, *Adopting a Risk-based Approach to Software and Hardware Security*
- 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 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*

Cybersecurity and Infrastructure Security Agency

- Binding Operational Directive (BOD) 26-04, *Prioritizing Security Updates Based on Risk*
- BOD 26-02, *Mitigating Risk From End-of-Support Edge Devices*
- 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 20-01, *Develop and Publish a Vulnerability Disclosure Policy*
- 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*

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

- Emergency Directive (ED) 26-03, Version 1, *Mitigate Vulnerabilities in Cisco SD-WAN Systems*
- ED 26-01, *Mitigate Vulnerabilities in F5 Devices*
- ED 25-03, Version 1, *Identify and Mitigate Potential Compromise of Cisco Devices*
- ED 25-02, *Mitigate Microsoft Exchange Vulnerability*
- ED 24-01, *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*

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

Appendix I: Status of Prior-Year Recommendations

The following table provides the status of the FY 2024 and FY 2025 FISMA performance audit recommendations.

Table 4: FY 2024 and FY 2025 FISMA Performance Audit Recommendations

Recommendation Number	Audit Recommendations	Auditor's Position on the Status
FY 2024 Audit Report A DFC 24 005 C		
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.[17]	Remain Open. Refer to Audit Results – Incident Response domain.
FY 2025 Audit Report A DFC 25 005 C		
1	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.	Remain Open. Refer to Audit Results – Risk and Asset Management, and Data Protection and Privacy domains.
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.	Closed. Refer to Audit Results – ISCM domain.
3	Document the independence of the assessment team in the risk assessment, including organizational relationships, contract structures (if applicable), and oversight arrangements.	Closed. Refer to Audit Results – ISCM domain.
4	Ensure the risk assessment is reviewed and approved by an Authorizing Official prior to the commencement of any assessment activity.	Closed. Refer to Audit Results – ISCM domain.

[17] OMB Memorandum M-21-31 was rescinded by OMB Memorandum M-26-14, *Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats*, issued May 22, 2026. RMA will evaluate closure of this recommendation based on the applicable successor requirements established under M-26-14.

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

Appendix II: Management's Response

DFC U.S. International Development Finance Corporation

1100 New York Avenue, NW
Washington, DC 20527
Office +1 202.336.8400
dfc.gov

Management Comments on Official Draft Report
DFC FY 2026 FISMA Performance Audit (Report No. DFC-26-005-C)

September 21, 2026

To: DFC Office of Inspector General
From: Willie Williams, Vice President and Chief Information Officer
Subject: Management Comments on Official Draft Report - DFC FY 2026 FISMA Performance Audit (Report No. DFC-26-005-C)

1. Overall Management Position

United States International Development Finance Corporation (DFC) appreciates the opportunity to review the Office of Inspector General's official draft report, "DFC's Fiscal Year 2026 Federal Information Security Modernization Act of 2014 Performance Audit" (Report No. DFC-26-005-C).

DFC agrees with the report's overall conclusion that DFC's information security program and practices were effective in FY 2026 and achieved a maturity level of Managed and Measurable under the FY 2025 IG FISMA Reporting Metrics v2.0.

DFC agrees with all eight recommendations. Management's responses, target implementation dates, and points of contact are provided below.

2. Management Response to Recommendations

Recommendation 1: Update the Asset Management Policy and Procedures and implement procedures for timely tracking of all assets, including those pending return, in storage, or for disposal.

- **Management Position:** Agree
- **Target Implementation Date:** November 30, 2026
- **Point of Contact:** Imran Shah, Director of IT Operations (OIT)
- **Management Response:** DFC will update Asset Management Policy and Procedures and implement procedures for timely tracking of all assets, including those pending return, in storage, or for disposal.

Recommendation 2: Review and dispose of long-term stored assets and ensure all devices are securely wiped prior to disposal.

- **Management Position:** Agree
- **Target Implementation Date:** November 30, 2026
- **Point of Contact:** Imran Shah, Director of IT Operations (OIT)
- **Management Response:** DFC will review and dispose of long-term stored assets and ensure all devices are securely wiped prior to disposal.

Recommendation 3: Establish thresholds and escalation procedures for aging inventory.

- **Management Position:** Agree
- **Target Implementation Date:** November 30, 2026
- **Point of Contact:** [redacted], IT Asset Manager (OIT)
- **Management Response:** DFC will establish thresholds and escalation procedures for aging inventory.

Recommendation 4: Implement validation controls to ensure accurate recording of asset details (e.g., type, model, serial number, asset tag).

- **Management Position:** Agree
- **Target Implementation Date:** November 30, 2026
- **Point of Contact:** [redacted], IT Asset Manager (OIT)
- **Management Response:** DFC will implement validation controls to ensure accurate recording of asset details (e.g., type, model, serial number, asset tag).

Recommendation 5: Restrict and monitor updates to asset records and enforce dual authorization for implementing significant status changes (e.g., disposal, availability).

- **Management Position:** Agree
- **Target Implementation Date:** November 30, 2026
- **Point of Contact:** Trevor Lowing, Chief Information Security Officer (OIT)
- **Management Response:** DFC will restrict and monitor updates to asset records and enforce dual authorization for implementing significant status changes (e.g., disposal, availability).

Recommendation 6: Ensure all hardware, including hardware that does not contain data, is consistently tagged with unique identifiers.

- **Management Position:** Agree

- **Target Implementation Date:** November 30, 2026
- **Point of Contact:** [redacted], IT Asset Manager (OIT)
- **Management Response:** DFC will ensure all hardware, including hardware that does not contain data, is consistently tagged with unique identifiers.

Recommendation 7: Perform a comprehensive physical inventory count and reconcile all hardware assets with the third-party service provider inventory system.

- **Management Position:** Agree
- **Target Implementation Date:** November 30, 2026
- **Point of Contact:** [redacted], IT Asset Manager (OIT)
- **Management Response:** DFC will perform a comprehensive physical inventory count and reconcile all hardware assets with the third-party service provider inventory system.

Recommendation 8: Implement a centralized tracking mechanism (e.g., compliance tracker, GRC tool, or calendar-based system) to monitor key milestones, due dates, and approvals.

- **Management Position:** Agree
- **Target Implementation Date:** November 30, 2026
- **Point of Contact:** [redacted], COOP Program Manager (Office of the Chief Policy Officer (OCPO))
- **Management Response:** DFC will implement a centralized tracking mechanism to monitor key milestones, due dates, and approvals for COOP governance activities.

3. FOIA Sensitivity Note

DFC has separately provided FOIA sensitivity input to OIG and requests limited redaction only for specific technical details that could reasonably increase cybersecurity risk if publicly disclosed (for example, precise counts and item-level descriptions of missing/unsanitized devices, and detailed descriptions of logging capability gaps). DFC does not request redaction of high-level findings, conclusions, or recommendation language.

If you have any questions regarding these comments, please contact the DFC Office of the Chief Information Officer.

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

DFC | U.S. International Development Finance Corporation

1100 New York Avenue, NW
Washington, DC 20527
Office +1 202.336.8400
dfc.gov

WILLIE WILLIAMS

Digitally signed by WILLIE WILLIAMS
Date: 2026.09.21 16:37:18 -04'00'

Willie Williams
Vice President and Chief Information Officer
U.S. International Development Finance Corporation

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

Appendix III: Evaluation of Management's Response

In response to the draft report, DFC's comments are included in **Appendix II**: Management's Response. Management indicated that the target implementation date to address FY 2026 – Recommendations 1 to 8 is November 30, 2026.

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.

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

Appendix IV: Glossary of Acronyms

BIA	Business Impact Analysis
BOD	Binding Operational Directive
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COOP	Continuity of Operations Plan
C-SCRM	Cybersecurity Supply Chain Risk Management
CSF	Cybersecurity Framework
DFC	U.S. International Development Finance Corporation
DHS	Department of Homeland Security
ED	Emergency Directive
FIPS	Federal Information Processing Standards
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
OIT	Office of Information Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RMA	RMA Associates, LLC
SCRM	Supply Chain Risk Management
SP	Special Publication
ZTA	Zero Trust Architecture