OFFICE OF INSPECTOR GENERAL

U.S. International Development Finance Corporation

Fiscal Year 2023 DFC Federal Information Security Modernization Act of 2014 Audit

October 2, 2023
Audit Report DFC-24-001-C

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

IMPORTANT NOTICE

This audit report contains sensitive but unclassified information that was redacted for public release for risk mitigation purposes.

Report Highlights

Office of Inspector General
International Development Finance Corporation

Fiscal Year 2023 DFC Federal Information Security Modernization Act of 2014 Audit

What Was Reviewed

The U.S. International Development Finance Corporation Office of Inspector General (OIG) contracted with the independent public accounting firm RMA Associates, LLC (RMA) to conduct the *Federal Information Security Modernization Act of 2014* (FISMA) audit of the United States International Development Finance Corporation (DFC) for Fiscal Year (FY) 2023 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 outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics.*

Our objectives were 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 outlined in the *FY 2023 - 2024 IG FISMA Reporting Metrics.*

What Was Found

In its audit of DFC, RMA determined DFC's information security program and practices were effective for FY 2023, 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 in the configuration management and the information security continuous monitoring domains. DFC made considerable progress from the prior year, as the prior year maturity level was Defined (Ineffective).

Recommendations

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

- **Recommendation 1**: We recommend that the DFC Chief Information Officer prioritize its efforts to enhance DFC's existing vulnerability management process to ensure sufficient identification, prioritization, and remediation of critical and high vulnerabilities in a timely manner in accordance with DFC's policy.
- **Recommendation 2**: We recommend that the DFC Chief Information Officer implement the necessary oversight to monitor Cybersecurity Security Assessment and Management (CSAM) to ensure that SSPs are reviewed and authorized in accordance with the timeliness requirements in DFC's policy.

MEMORANDUM:

DATE: October 2, 2023

TO: MS. TINA DONBECK
CHIEF INFORMATION OFFICER (CIO)

FROM: Mr. Anthony "Tony" Zakel
Inspector General

SUBJECT: Fiscal Year 2023 DFC Federal Information Security Modernization Act of 2014 Audit (Report Number DFC-24-001-C)

We contracted with the independent public accounting firm of RMA Associates LLC (RMA) to audit DFC's Fiscal Year 2023 Federal Information Security Modernization Act of 2014 Audit. The contract included reporting on 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 FY 2023 supplemental metrics outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics*. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards (GAGAS), Office of Management and Budget (OMB) M-10-15, and Circular No. A-130, Section 522 of the Consolidated Appropriations Act of 2005, and others such as National Institute of Standards and Technology (NIST).

In its audit of DFC, RMA concluded that DFC's information security program and practices were effective for FY 2023, as DFC's information security program met the criteria required to be assessed at a maturity level of Managed and Measurable. RMA's tests of the information security program identified two findings that fell in the configuration management and the information security continuous monitoring domains. RMA made two recommendations to assist DFC in strengthening its information security program. Further, all nine prior FISMA performance audit recommendations were closed.

RMA is responsible for the attached auditor's report dated October 2, 2023, and the conclusions expressed therein. We do not express opinions on DFC's information systems or internal control over information systems, or on whether DFCs information systems complied with FISMA, or conclusion on compliance or any other matters.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact me at 202-873-6422.

Anthony "Tony" Zakel
Inspector General
U.S. International Development Finance Corporation

CC: Chief Executive Officer
Deputy Chief Executive Officer
Chief Operating Officer
Chief Risk Officer
All Vice Presidents
Director of Internal Audits
RMA Associates

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
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 2023

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

October 2, 2023

Anthony Zakel, 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 2023

Dear Mr. Zakel:

RMA Associates, LLC is pleased to submit our Performance Audit on the effectiveness of the United States International Development Finance Corporation's (DFC) Information Security Program and Practices Report for Fiscal Year (FY) 2023. 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 what maturity level DFC achieved for each of the core metrics and FY 2023 supplemental metrics outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics*.

Based on the results of our performance audit, we determined that DFC's information security program and practices were effective for FY 2023, as DFC's information security program met the criteria required to be assessed at a maturity level of Managed and Measurable. Our tests of the information security program identified two findings that fell in the configuration management and the information security continuous monitoring domains. We made two recommendations to assist DFC in strengthening its information security program. Further, all nine prior FISMA performance audit recommendations were closed.

Additionally, our report includes *Appendix I: Status of Prior Year Recommendations*, *Appendix II: Management Responses*, and *Appendix III: Evaluation of Management Responses*.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, which 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objectives.

We have also prepared the answers to the Office of Management and Budget's FY 2023 Inspector General Metrics (February 2023). These metrics provide reporting requirements across functional areas to be addressed in the independent assessment of agencies' information security programs.

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

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

Sincerely,

Reza Mahbod

Reza Mahbod
President

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Inspector General
United States International Development Finance Corporation

RMA Associates LLC (RMA) conducted a performance audit of the effectiveness of the United States International Development Finance Corporation's (DFC) information security program and practices for fiscal year (FY) 2023. We conducted our performance audit for FY 2023 as of July 31, 2023. The performance audit fieldwork covered DFC's headquarters in Washington, DC, from February 1, 2023, to August 28, 2023.

In accordance with the *Federal Information Security Modernization Act of 2014* (FISMA),[1] 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 DFC achieved for each of the core metrics and FY 2023 supplemental metrics outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics*.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards (GAGAS)*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions based on our performance audit objective. We believe that the evidence obtained provides a reasonable basis for determining the maturity level for the core and supplemental metrics and conclusions based on our performance 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) guidance and we assessed selected security controls outlined in *NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations*. We assessed four internal and external systems out of a total of four FISMA reportable systems from DFC's FISMA inventory of information systems.

For FY 2023, OMB required Inspector Generals to assess 40 of the 66 metrics from the *FY 2021 IG FISMA Reporting Metrics v1.1* (May 12, 2021), including the core metrics and supplemental metrics of Group 1, a combination of metrics that must be evaluated on a two-year calendar basis and agreed to by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the Chief Information Security Officer, OMB, and Cybersecurity & Infrastructure Security Agency (CISA). The FY 2023 IG Metrics were aligned with the five following Cybersecurity Framework security functions areas: Identify, Protect, Detect, Respond, and Recover to determine the effectiveness of agencies' information security program. The FY 2023 IG Metrics classifies information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

We determined that DFC implemented an effective information security program by achieving an overall Managed and Measurable maturity level based on the *FY 2023 - 2024 IG FISMA Reporting Metrics*. Our tests of the information security program identified two findings that fell in the configuration management and the information security continuous monitoring domains. We made two recommendations to assist DFC in strengthening its information security program. Further, there were no recommendations from prior FISMA performance audits that remain open.

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 status. The information included in this report was obtained from DFC on or before July 31, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring after July 31, 2023.

Additional information on our findings and recommendations is included in the accompanying report.

Respectfully,

RMA Associates

RMA Associates, LLC
Arlington, VA

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Table of Contents

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Introduction

This report presents the results of RMA Associates, LLC (RMA) 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)[2] requires Federal agencies to have an annual independent performance audit or evaluation of 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) for the collection of 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 in support of 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 what maturity level DFC achieved for each of the core metrics and Fiscal Year (FY) 2023 supplemental metrics outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics*.

As part of our performance audit, we responded to the FY 2023 20 core and 20 supplemental metrics specified in OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics*, dated February 10, 2023.[3] These metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs.[4] 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 (BUILD Act),* 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 (OPIC) and the U.S. Agency for International Development's (USAID) Development Credit Authority (DCA).

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

[2] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).
[3] 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.
[4] Refer to the section titled, *Objective, Scope, and Methodology,* for more details.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

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 information 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* (known as the Clinger-Cohen Act), explicitly emphasizes a risk-based policy for 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 responsibility;
- Periodically review the security controls in its systems; and
- Authorize system processing prior to operations and periodically after that.

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

FISMA provided OMB oversight authority of agency security policies and practices and provided authority for implementing agency policies and practices for information systems to DHS.[5]

FISMA required the Secretary of DHS to develop and oversee the implementation of operational directives requiring agencies to implement OMB's standards and guidelines for safeguarding federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. FISMA directed the Secretary to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security

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

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

standards.[6] It authorized the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.[7]

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 (GAO). The reports is required to include: (1) threats and threat factors, vulnerabilities, and impacts of the incidents; (2) risk assessments of affected systems before the incidents; (3) the status of compliance of the systems at the time of the incidents; (4) detection, response, and remediation actions; (5) the 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.[8]

Key Changes to the Metrics

One of the annual FISMA evaluation goals was to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, on December 2, 2022, that provides guidance on how OMB and Council of the Inspectors General on Integrity and Efficiency (CIGIE) are transitioning the IG metrics process to a multi-year cycle and other guidance, such as directing federal agencies to increase their Continuous Diagnostics and Mitigation implementation efforts. Using a multi-year cycle, a core group of metrics must be evaluated annually, and the remainder of the standards and controls will be evaluated in metrics on a 2-year cycle. The multi-year cycle approach was agreed to by CIGIE, OMB, the federal Chief Information Security Officer (CISO) Council, and DHS's Cybersecurity & Infrastructure Security Agency (CISA).

As a representation of this guidance, on February 10, 2023, the final IG FISMA Metrics for FY 2023 were released,[9] which included the 20 core metrics plus an additional 20 supplemental metrics to be assessed in the FY 2023 review cycle. The remaining supplemental metrics will be tested along with the core metrics as part of the FY 2024 review cycle.

Additionally, OMB Memorandum M-23-03 solidifies the timeline adjustment for the IG evaluation of agency effectiveness to align the evaluation results with the budget submission cycle to facilitate the timely funding for the remediation of problems identified. Historically, IG evaluation of agency effectiveness finished in October until FY 2022, when the deadline shifted to July 31 of each year. However, OMB granted DFC OIG an extension to submit the FY 2022 IG CyberScope results by September 30, 2022. For FY 2023, the IG evaluation had a deadline of July 31, 2023, for FISMA reporting to OMB and DHS and this deadline was met.

Finally, in previous years, IGs were directed to utilize a mode-based scoring approach to assess agency maturity levels. Under this approach, ratings throughout the reporting domains were

[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] DHS, *FY 2023 – 2024 IG FISMA Reporting Metrics* (February 10, 2023).

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

determined by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the domain rating. The same logic was applied to the function and overall information security program level. However, OMB and CIGIE determined this was not the best approach. The approach for FY 2023 focused on a calculated average approach (instead of mode), wherein IGs used the average of the metrics in a particular domain to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program.

Core and FY 2023 Supplemental IG Metrics

OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics* Version 1.1, dated February 10, 2023, specified the FY 2023 20 Core and 20 Supplemental IG Metrics. It directed IGs to report the assessed maturity levels of these metrics in CyberScope no later than July 31, 2023. The FY 2023 FISMA IG Metrics were aligned with the five Cybersecurity Framework security function areas (key performance areas) as follows:

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

We evaluated 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 2023 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.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

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.

In FY 2023, a calculated average scoring model was used, where core and supplemental metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. For example, if the calculated core metric maturity of two of the function areas is Level 3: Consistently Implemented (i.e., 3.0) and the computed core metric maturity of the remaining three function areas is Level 4: Managed and Measurable (i.e., 4.0), the information security program rating would average to be 3.60 (i.e., (3+3+4+4+4)/5).

We focused on the results of the core metrics to determine maturity levels and 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 4.36, the Managed and Measurable level. As a result, DFC's overall assessed maturity level was effective.

DFC's FY 2023 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 2023.**

Table 2: Overall Calculated Averages Maturity Calculation in FY 2023

Function	Core Metrics	FY 2023 Supplemental Metrics	FY 2023 Assessed Maturity Average[10]	FY 2023 Assessed Maturity
Identify	4.33	4.00	4.17	Managed and Measurable
Protect	4.50	4.30	4.40	Managed and Measurable
Detect	3.00	5.00	4.00	Managed and Measurable
Respond	4.50	5.00	4.75	Managed and Measurable

[10] The FY 2023, 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.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Function	Core Metrics	FY 2023 Supplemental Metrics	FY 2023 Assessed Maturity Average[10]	FY 2023 Assessed Maturity
Recover	4.50	4.50	4.50	Managed and Measurable
Calculated Maturity	**4.17**	**4.56**	**4.36**	**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 five Cybersecurity Functions[11] and nine FISMA Metric Domains.[12] 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 2023.

We provided the DFC with a draft of this report for 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 1 and 2 is October 31, 2023 (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).

DFC made considerable progress in implementing prior recommendations, some dating back to 2017. During FY 2023, DFC resolved all nine open recommendations from the FY 2017 to FY 2022 FISMA audits, yielding significant improvements in IG FISMA Metrics results. **Appendix I: Status of Prior Year Findings** provides the summary of the status of prior year recommendations.

However, we did identify weaknesses in DFC's security posture in preserving the agency's information and information systems' confidentiality, integrity, and availability. [redacted] We made two 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. We noted that DFC made considerable progress from the prior year, as the prior year maturity level was Defined (Ineffective).

[11] OMB, DHS, and CIGIE developed the FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The nine FISMA Metric Domains were aligned with the five functions: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[12] As described in the FISMA Reporting Metrics, the nine FISMA Metric Domains are: (1) risk management, (2) supply chain risk management (SCRM) (3) configuration management, (4) identity and access management, (5) data protection and privacy, (6) security training, (7) information security continuous monitoring (ISCM), (8) incident response, and (9) contingency planning.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

DFC's maturity and effectiveness levels have increased from the prior year and are presented in **Table 3: FY 2022 – FY 2023 Maturity Level Comparison**.

Table 3: FY 2022 – FY 2023 Maturity Level Comparison

Function	FY 2022 Assessed Maturity	FY 2023 Assessed Maturity
Identify	Defined	Managed and Measurable
Protect	Optimized	Managed and Measurable
Detect	Defined	Managed and Measurable
Respond	Optimized	Managed and Measurable
Recover	Defined	Managed and Measurable
Overall Maturity	**Defined**	**Managed and Measurable**
Overall Effectiveness	**Not Effective**	**Effective**

The maturity level for the nine domains is presented below in **Table 4: The DFC's FY 2023 Maturity Levels**:

Table 4: The DFC's FY 2023 Maturity Levels

Function	Maturity Level	
Function 1: Identify		Managed and Measurable (Level 4)
• Risk Management	Managed and Measurable (Level 4)	
• Supply Chain Risk Management	Managed and Measurable (Level 4)	
Function 2: Protect		Managed and Measurable (Level 4)
• Configuration Management	Consistently Implemented (Level 3)	
• Identity Management	Managed and Measurable (Level 4)	
• Data Protection and Privacy	Managed and Measurable (Level 4)	
• Security Training	Managed and Measurable (Level 4)	
Function 3: Detect—Information Security Continuous Monitoring		Managed and Measurable (Level 4)
Function 4: Respond—Incident Response		Managed and Measurable (Level 4)
Function 5: 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 provide the Chief Information Officer with recommendations to remediate deficiencies.

Risk Management

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

DFC implemented its security architecture across the enterprise, business process, and system levels to help leadership make informed risk management decisions. Those risk management

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

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 consistently captured and shared lessons learned on the effectiveness of risk management processes and activities to update the program. Information system inventory, hardware, and software assets inventory were maintained comprehensively and accurately. Further, DFC implemented a plan to decommission the unsupported software within DFC's network per last year's FISMA report finding.[13] Hence, we determined FY 2022-Recommendation 2 is closed.[14] Our overall assessment 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 management controls in place were overall effective.

Supply Chain Risk Management (SCRM)

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

DFC developed and implemented the SCRM strategy, policies, and procedures to manage supply chain risks with suppliers, contractors, and systems. In addition, DFC monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its 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. Hence, we determined FY 2021-Recommendation 3 is closed.[15] Our overall assessment for this domain determined 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 SCRM controls in place were overall effective.

Configuration Management

We determined the DFC's overall maturity level for the Configuration Management program was Consistently Implemented. [redacted]

DFC Must Improve its Vulnerability and Patch Management Controls

According to the Office of Information Technology (OIT) *Vulnerability and Posture Management Guide* version 1.1, vulnerabilities rated as "Critical and High" are required to be remediated within 30 days of initial detection. In addition, the NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* requires organizations must resolve their system flaws systematically and improve the security and integrity of their

[13] FY 2022 FISMA Audit Report A-DFC-23-001-C
[14] Ibid.
[15] FY 2021 FISMA Audit Report A-DFC-22-003-C

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

software and firmware. It involves testing updates related to flaw remediation for effectiveness and potential side effects before installation. In addition, security-relevant updates must be installed within a specified time period after release, and flaw remediation is integrated into the organizational configuration management process to ensure proper documentation and tracking of fixes.

Our FY 2023 FISMA performance audit noted a decrease in the number of DFC's vulnerabilities, as DFC was consistently removing and decommissioning the OPIC systems from their network. Although DFC improved its Vulnerability Management Program, further improvement needs to be made. [redacted]

[redacted]

Timely remediation of vulnerabilities is critical to ensuring the risk that mission information or other sensitive data may be inadvertently or deliberately misused is minimized. Such misuse may result in improper information disclosure, manipulation, or theft. Additionally, vulnerabilities that are not corrected may lead to inappropriate or unnecessary changes to mission-focused information systems, which could result in the compromise of mission information or other sensitive data.

This issue was also mentioned in the previous FISMA performance audit reports,[16] and DFC had made progress in decommissioning OPIC systems. The number of vulnerabilities decreased, and no vulnerabilities existed from 2017 and 2018. Hence, we determined FY 2017- Recommendation 1 and FY 2018-Recommendation 2 and 3 are closed. However, we are making a new recommendation to address the vulnerability issue for FY 2023.

> **Recommendation 1**: We recommend that the DFC Chief Information Officer prioritize its efforts to enhance DFC's existing vulnerability management process to ensure sufficient identification, prioritization, and remediation of critical and high vulnerabilities in a timely manner in accordance with DFC's policy.

Identity and Access Management

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

[redacted] All of the organization's systems interface with the solution to oversee employees, resulting in an ability to manage user (non-privileged)

[16] FY 2017 FISMA Audit Report A-OPC-17-007-C and FY 2018 FISMA Audit Report A-OPC-19-006-C

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

accounts and privileges centrally and report on the effectiveness on a near real-time basis. [redacted] Additionally, DFC utilized lessons learned, end users' devices were properly configured, and privileged users utilized a strong authentication mechanism. Hence, we determined FY 2020-Recommendation 3 is closed.[17] Our overall assessment for this domain determined 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 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 Managed and Measurable.

DFC's systems were approved to collect and process Personally Identifiable Information (PII). The controls over PII were the responsibility of the 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 annual exfiltration exercise to measure the effectiveness of its data exfiltration and enhanced network defenses. Testing performed by the independent auditors found no exceptions for data protection and privacy, and the controls were operating as intended. We determined DFC's Data Protection and Privacy controls in place were effective.

Security Training

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

DFC performed roles and responsibilities for security training, completed workforce assessment, and annual security training. DFC effectively allocated resources in a risk-based manner for stakeholders to implement security awareness training consistently. DFC also was able to demonstrate the ability to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. In addition, DFC addressed its identified knowledge, skills, and abilities gaps through talent acquisition. Our testing found no exceptions for security training, 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 Security Training controls in place were overall effective.

Information Security and Continuous Monitoring

[17] FY 2020 FISMA Audit Report A-DFC-21-005-C

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

We determined the DFC's overall maturity level for the ISCM program was Managed and Measurable. We found one weakness in the ISCM domain regarding reviewing and authorizing system-level SSP.

DFC Must Sign and Approve its System-Level System Security Plans (SSP)

According to the NIST SP 800-53, Revision 5 emphasizes the importance of developing security and privacy plans for federal information systems and organizations. These plans need to be reviewed and approved by the appropriate authority before implementation. Additionally, the plans should be regularly reviewed and updated to address any changes to the system, environment of operation, or problems identified during the implementation or control assessments. OIT *Continuous Monitoring Plan* version 5.1[18] also requires SSPs to be reviewed annually and updated when necessary. Additionally, System Owners (SO) /Information System Security Officers are required to perform annual SSP reviews and signoffs. [redacted]

DFC did not have an adequate monitoring mechanism to ensure system-level SSPs' timely review and approval. After inquiring with DFC management, both SSPs were signed by the SO and Authorizing Official on June 1, 2023.

Without consistently reviewing and authorizing the SSPs for DFC systems, the authorizing official and other agency stakeholders may not be aware of security and privacy risks to the systems, potentially impacting the overall risk exposure to DFC.

> **Recommendation 2**: We recommend that the DFC Chief Information Officer implement the necessary oversight to monitor Cybersecurity Security Assessment and Management (CSAM) to ensure that SSPs are reviewed and authorized in accordance with the timeliness requirements in DFC's policy.

Although two out of four selected systems for testing had SSPs that were not authorized and signed, DFC regularly analyzed performance metrics to adjust and improve its program. In addition, DFC's resources were allocated in a risk-based manner for stakeholders to implement ISCM activities effectively. DFC transitioned to ongoing control and system authorization by implementing its continuous monitoring policies and strategy. DFC updated its Authorization to Operate and system-level Security Assessment Reports annually. Further, DFC documented and implemented lessons learned to enhance the continuous monitoring process to instruct employees to record, analyze, and revise control activities on a cyclical basis to continuously improve DFC security posture as defined in the Security Continuous Monitoring Plan. Hence, we determined FY 2022-Recommendation 1 and 3 are closed.[19] Our overall control testing for this domain determined the controls were operating as intended. Consequently, based on DFC's overall

[18] OIT *Continuous Monitoring Plan* version 5.1 (01/19/2023)
[19] FY 2022 FISMA Audit Report A-DFC-23-001-C

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

implementation of security controls and considering the unique mission, resources, and challenges of DFC, 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.

The DFC performed tabletop exercises yearly to evaluate the implementation of its incident response policies, and it was found through these exercises that the policies were effective. [redacted] We determined the DFC's Incident Response program controls in place were effective.

Contingency Planning

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

DFC's resources (people, processes, and technology) were allocated in a risk-based manner for stakeholders to implement system contingency planning activities effectively. In addition, system-level Business Impact Analyses (BIAs) 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. DFC ensured that the data supporting the metrics were obtained accurately, consistently, and in a reproducible format. Hence, we determined FY 2022-Recommendation 5 is closed.[20] Our assessment of this domain found no exceptions and determined the controls were operating as intended. We determined the DFC's Contingency Planning controls in place were effective.

Overall Conclusion

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we determined the DFC's information security program and practices were established. They were maintained for the five Cybersecurity Functions and nine FISMA Metric

[20] FY 2022 FISMA Audit Report A-DFC-23-001-C

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Domains. We determined the DFC's information security program and practices were effective for FY 2023, 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 in the configuration management and the information security continuous monitoring domains. We made two recommendations to assist DFC in strengthening its information security program. Further, all nine prior FISMA performance audit recommendations were closed.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

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 FY 2023 supplemental metrics outlined in the *FY 2023 – 2024 IG FISMA Metrics*. Specifically, the performance audit determined whether DFC implemented an effective information security program by evaluating the five Cybersecurity Framework security functions as divided into nine domains:

- **Identify**, which includes questions pertaining to risk management and supply chain risk management;
- **Protect**, which includes questions pertaining to configuration management, identity, and access management, data protection and privacy, and security training;
- **Detect**, which includes questions pertaining to information security continuous monitoring;
- **Respond**, which includes questions pertaining to incident response; and
- **Recover**, which includes questions 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 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 that we conducted was DFC agency-wide, and the review was for FY 2023 as of July 31, 2023. [redacted] The performance audit fieldwork covered DFC's headquarters in Washington, DC, and audit work was conducted between February 1 and August 28, 2023. The performance audit included steps to follow up on prior year deficiencies.

Methodology

The overall strategy of our evaluation considered the following: (1) National Institute of Standards and Technology (NIST) Special Publication (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 Federal Information Systems and Organizations;* (3) *FY 2023-2024 IG FISMA Reporting Metrics*; and (4) the DFC's policies and procedures.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

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. Also, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

In testing for the effectiveness of the security controls relevant to the 20 core metric questions and 20 FY 2023 supplemental metric questions specified in OMB's *FY 2023 – 2024 IG FISMA Metrics*, we tested the entire population of administrative controls of the DFC. The application controls were the responsibility of the DFC's service providers.

We focused our FY 2023 FISMA audit approach on Federal information security guidelines developed by the DFC, NIST, and OMB. The following is a listing of the criteria used in the performance of the FY 2023 FISMA audit:

NIST Federal Information Processing Standards (FIPS) Publications and SPs

- 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 800-50, *Building an Information Technology Security Awareness and Training Program*
- 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*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*
- 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 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*
- 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

- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*
- 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-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

- 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 Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

DHS Directives and Other Guidance

- *FY 2023 – 2024 IG FISMA Reporting Metrics*
- Binding Operational Directive 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- DHS Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- DHS Emergency Directive 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- DHS Emergency Directive 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*
- DHS Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*
- DHS Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*
- DHS Emergency Directive 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*
- DHS Emergency Directive 20-03, *Mitigate Windows Domain Name System (DNS) Server Vulnerability from July 2020 Patch Tuesday*
- DHS Emergency Directive 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- DHS Binding Operational Directive 20-01, *Develop and Publish Vulnerability Disclosure Policy*
- DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*
- DHS Binding Operational Directive 18-02, *Securing High-Value Assets*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

- DHS Binding Operational Directive 18-01, *Enhance Email and Web Security*
- DHS Binding Operational Directive 17-01, *Removal of Kaspersky-branded Products*
- DHS Binding Operational Directive 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- DHS Binding Operational Directive 16-02, *Threat to Network Infrastructure Devices*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Abbreviations

BIA	Business Impact Analysis
BUILD Act	Better Utilization of Investments Leading to Development Act of 2018
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSAM	Cybersecurity Security Assessment and Management
DCA	Development Credit Authority
DFC	United States International Development Finance Corporation
DHS	Department of Homeland Security
DNS	Domain Name System
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
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
OPIC	Overseas Private Investment Corporation
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law
RMA	RMA Associates, LLC
SCRM	Supply Chain Risk Management
SO	System Owner
SP	Special Publication
SSP	System Security Plan
TIC	Trusted Internet Connection
USAID	United States Agency for International Development

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Appendix I: Status of Prior Year Recommendations

The following table provides the status of the FY 2022, FY 2021, FY 2020, FY 2018, & FY 2017 FISMA performance audit recommendations.

Table 5: FY 2022, 2021, 2020, 2018, & 2017 FISMA Performance Audit Recommendations

Recommendation No.	Audit Recommendations	DFC's Position	Auditor's Position on the Status
FY 2022 Audit Report A-DFC-23-001-C			
1	Update its Authorization to Operate and system-level Security Assessment Reports annually.	Closed	Agree. Refer to Audit Results – ISCM domain
2	[redacted]	Closed	Agree. Refer to Audit Results – Risk Management domain
3	[redacted]	Closed	Agree. Refer to Audit Results – ISCM domain
5	[redacted]	Closed	Agree. Refer to Audit Results – Contingency Planning domain
FY 2021 Audit Report A-DFC-22-003-C			
3	[redacted]	Closed	Agree. Refer to Audit Results – SCRM domain
FY 2020 Audit Report A-DFC-21-005-C			
3	[redacted]	Closed	Agree. Refer to Audit Results – Identity and Access Management domain
FY 2018 Audit Report A-OPC-19-006-C			
2	[redacted]	Closed	Agree. Refer to Audit Results – Configuration Management domain

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Recommendation No.	Audit Recommendations	DFC's Position	Auditor's Position on the Status
3	[redacted]	Closed	Agree. Refer to Audit Results – Configuration Management domain
FY 2017 Audit Report A-OPC-17-007-C			
1	[redacted]	Closed	Agree. Refer to Audit Results – Configuration Management domain

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Appendix II: Management Response

DFC U.S. International Development Finance Corporation

MEMORANDUM September 26, 2023

TO: Anthony Zakel
Inspector General
DFC – Office of the Inspector General

FROM: Tina Donbeck
Chief Information Officer

SUBJECT: Fiscal Year 2023 DFC Federal Information Security Modernization Act of 2014 Audit

The U.S. International Development Finance Corporation (DFC) management appreciates the report produced by the Office of the Inspector General (OIG) and RMA Associates. The corporation will use the RMA recommendations to improve and continue to strengthen its Information Security Program.

The FY23 Report recognizes that the Information Security Program of the U.S. International Development Finance Corporation made considerable progress over the prior year and is effective by rating "Managed and Measurable" for all six functional areas assessed. The agency will continue to incorporate further areas of improvement in its responsiveness to vulnerability management and will ensure resources are adequately allocated in the timely review of System Security Plans (SSP).

We appreciate the OIG for noting DFC's progress from past years audits to include the remediation and closure of all prior year findings dating back to 2017.

Thank you for the professionalism and courtesy that you and all your OIG personnel demonstrated throughout this review.

TINA DONBECK Digitally signed by TINA DONBECK Date: 2023.09.26 09:55:22 -04'00'

Tina Donbeck, Vice President and Chief Information Officer

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

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Appendix III: Evaluation of Management Response

In response to the draft report, DFC's comments are included in **Appendix II: Management Response**. In subsequent correspondence, DFC management indicated that the target implementation dates to address Fiscal Year (FY) 2023 - Recommendations 1 and 2 is October 31, 2023. Remediation efforts as well as System Security Plan (SSP) timeliness will be reenforced in FY 2024 Performance Plans.

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