OFFICE OF INSPECTOR GENERAL

U.S. International Development Finance Corporation

Fiscal Year 2024 DFC Federal Information Security Modernization Act of 2014 Audit

September 25, 2024
Audit Report DFC-24-005-C

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

Report Highlights

Office of Inspector General
International Development Finance Corporation

Fiscal Year 2024 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) 2024 to evaluate the effectiveness of the DFC's information security program and practices, and determine what maturity level DFC achieved for each of the core metrics and supplemental metrics outlined in the *FY 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 the maturity level DFC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2023 - 2024 IG FISMA Reporting Metrics.*

What Was Found

In this audit of DFC, RMA determined DFC's information security program and practices were effective for FY 2024, 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 incident response and contingency planning domains.

Recommendation

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

- **<u>Recommendation 1</u>**: We recommend that DFC's Chief Information Officer fully implement event logging requirements in accordance with Office of Management and Budget, Memorandum M-21-31.

Office of Inspector General

U.S. International Development Finance Corporation

MEMORANDUM:

Date: September 25, 2024

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

From: Mr. Anthony "Tony" Zakel
Inspector General

Subject: Fiscal Year 2024 DFC Federal Information Security Modernization Act of 2014 Audit (Report Number DFC-24-005-C)

The Office of Inspector General (OIG) contracted with the independent public accounting firm of 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) 2024 to evaluate the effectiveness of the DFC's information security program and practices, and determine what maturity level DFC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics*. The contract required RMA to perform the engagement in accordance with generally accepted government auditing standards (GAGAS), Office of Management and Budget (OMB) *FY 2023 – 2024 IG FISMA Reporting Metrics*, 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 reported the information security program and practices were effective for FY 2024, 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 incident response and contingency planning domains.

RMA is responsible for the attached auditor's report dated September 25, 2024 and the conclusions expressed therein. We do not express opinions on DFC's information systems or internal control over information systems, or on whether DFC's information systems complied with FISMA, or conclusions on compliance and 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: Scott Nathan (Chief Executive Officer)
Nisha Biswal (Deputy Chief Executive Officer)
Jane Rhee (Chief of Staff)
Jody Myers (Chief Risk Officer)
Keron White (Chief Administrative Officer)
Mildred Callear (Chief Financial Officer)
Agnes Dasewicz (Chief Operating Officer)
Dev Jagadesan (Deputy General Counsel)
John Glaser (Deputy Chief Information Officer)
Trevor Lowing (Chief Information Security Officer)
Eric Styles (Administrative Counsel)
Ryan Zalaskus (Managing Director Office of Financial and Portfolio Management)
RMA Associates

United States International Development Finance Corporation

Federal Information Security Modernization Act of 2014

Performance Audit Report for Fiscal Year 2024

RMA | Associates
Auditors. Consultants. Advisors.

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

September 25, 2024

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 2024

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) 2024. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objective of this performance audit was to evaluate the effectiveness of the DFC's information security program and practices and determine the maturity level DFC achieved for each of the core metrics and FY 2024 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 2024, 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 incident response and contingency planning domains. We made one recommendation to assist DFC in strengthening its information security program. Further, all two 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 2024 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.

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

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) 2024. We conducted our performance audit for FY 2024 as of July 31, 2024. The performance audit fieldwork covered DFC's headquarters in Washington, DC, from February 1, 2024, to July 31, 2024.

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 the maturity level DFC achieved for each of the core metrics and FY 2024 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 four FISMA reportable systems from DFC's FISMA inventory of information systems.

For FY 2024, OMB required Inspector Generals to assess 37 of the 66 metrics from the *FY 2021 IG FISMA Reporting Metrics v1.1* (May 12, 2021), including the core metrics and supplemental metrics. Supplemental metrics are 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 2024 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 2024

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

IG Metrics classifies information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

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 incident response and contingency planning domains. We made one recommendation to assist DFC in strengthening its information security program. Further, no recommendations from prior FISMA performance audits 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, 2024. We have no obligation to update our report or to revise the information contained therein to reflect events occurring after July 31, 2024.

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

Respectfully,

RMA Associates

RMA Associates, LLC
Arlington, VA

Table of Contents

Introduction 2

Background 2

United States International Development Finance Corporation 2

Federal Information Security Modernization Act of 2014 3

Key Changes to the Metrics 4

Core and FY 2024 Supplemental IG Metrics 5

Summary Performance Audit Results 6

Objective, Scope, and Methodology 16

Abbreviations 20

Appendix I: Status of Prior Year Recommendations 21

Appendix II: Management Response 22

Appendix III: Evaluation of Management Response 23

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 conduct 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 supporting the FISMA performance audit requirement. The objective of this performance audit was to evaluate the effectiveness of DFC's information security program and practices and determine the maturity level DFC achieved for each of the core metrics and Fiscal Year (FY) 2024 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 2024 20 core and 17 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 Development Credit Authority.

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

[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.

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

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*, required each Federal agency to develop, document, and implement an agency-wide program to provide 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 responsibilities;
- 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, that 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 that 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

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

developed by NIST to ensure operational directives do not conflict with NIST information security 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 report is required to include: (1) threats and threat actors, vulnerabilities, and impacts of the incidents; (2) risk assessments of affected systems before the incidents; (3) the status of 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-24-04,[9] *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, on December 4, 2023, which among other areas such as directs Federal agencies to increase their Continuous Diagnostics and Mitigation implementation efforts, and provides agencies with FY 2024 reporting guidance and deadlines in accordance with FISMA.[10]

As a representation of this guidance, on February 10, 2023, the final *FY 2023 – 2024 IG FISMA Reporting Metrics* were released,[11] which included the 20 core metrics plus an additional 17 supplemental metrics to be assessed in the FY 2024 review cycle. The FY 2024 IG Metrics are based on coordinated discussions between (and the consensus opinion of) representatives from OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch Chief Information Security Officers (CISO) and their staff, the Intelligence Community, and among other OIGs throughout the Federal government included in an established working group.[12]

OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, also solidifies the timeline adjustment for the IG evaluation of agency effectiveness to align the results with the budget submission cycle. Historically, IG's evaluation of agency effectiveness finished in October until FY 2022, when the deadline shifted to July 31st of each year unless an extension was granted to September 30, 2022. For FY 2024, the

[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] M-24-04 *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, December 4, 2023.
[10] 44 U.S.C. §§ 3551 et seq.
[11] *FY 2023 – 2024 IG FISMA Reporting Metrics* (February 10, 2023).
[12] CISO Council FISMA Metrics Subcommittee.

IG evaluation has a deadline of July 31, 2024, for FISMA reporting to OMB and DHS to align the release of IG assessments to better facilitate the timely funding for the remediation of problems identified. The previous timing limited agency leadership's ability to request resources in the next Budget Year submissions for remediations.

Core and FY 2024 Supplemental IG Metrics

OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics* Version 1.1, dated February 10, 2023, specified the FY 2024 20 Core and 17 Supplemental IG Metrics. It directed IGs to report the assessed maturity levels of these metrics in CyberScope no later than July 31, 2024. The FY 2024 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 2024 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.

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 2024, 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 4.46, the Managed and Measurable level. As a result, DFC's overall assessed maturity level was effective.

DFC's FY 2024 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 2024.**

Table 2: Overall Calculated Averages Maturity Calculation in FY 2024

Function	Core Metrics	FY 2024 Supplemental Metrics	FY 2024 Assessed Maturity Average[13]	FY 2024 Assessed Maturity
Identify	4.50	4.67	4.58	Managed and Measurable
Protect	4.75	4.38	4.56	Managed and Measurable
Detect	5.00	5.00	5.00	Optimized
Respond	4.00	4.33	4.17	Managed and Measurable
Recover	4.50	3.50	4.00	Managed and Measurable
Calculated Maturity	**4.55**	**4.38**	**4.46**	**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[14] and nine FISMA Metric

[13] The FY 2024, 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.

[14] 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*.

Domains.[15] 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 2024.

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 recommendation 1 is December 2025 (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. During FY 2024, DFC resolved all two open recommendations from the FY 2023 FISMA audits, yielding significant improvements in IG FISMA Metrics results. **Appendix I: Status of Prior Year Findings** provides a summary of the status of recommendations from the prior year.

However, we did identify weaknesses in DFC's security posture in preserving the agency's information and information systems' confidentiality, integrity, and availability. Consequently, we noted weaknesses in two IG FISMA Metric Domains: DFC did not reach the event logging requirements at the Event Logging tier level (EL3) in accordance with OMB M-21-31, and DFC did not authorize the Continuity of Operations Plan (COOP) nor integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related business process continuity plans to deliver persistent situational awareness across the organization. We made one recommendation 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.

DFC's maturity and effectiveness levels have increased from the prior years and are presented in **Table 3: FY 2022 – FY 2024 Maturity Level Comparison**.

Table 3: FY 2022 – FY 2024 Maturity Level Comparison

Function	FY 2022 Assessed Maturity	FY 2023 Assessed Maturity	FY 2024 Assessed Maturity
Identify	Defined	Managed and Measurable	Managed and Measurable
Protect	Optimized	Managed and Measurable	Managed and Measurable
Detect	Defined	Managed and Measurable	Optimized
Respond	Optimized	Managed and Measurable	Managed and Measurable
Recover	Defined	Managed and Measurable	Managed and Measurable
Overall Maturity	**Defined**	**Managed and Measurable**	**Managed and Measurable**
Overall Effectiveness	**Not Effective**	**Effective**	**Effective**

[15] 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.

The maturity level for the nine domains is presented below in **Table 4: The DFC's FY 2024 Maturity Levels:**

Table 4: The DFC's FY 2024 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	Managed and Measurable (Level 4)	
• 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		Optimized (Level 5)
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 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 employed automated systems to track the lifecycle of hardware assets connected to the network, including mobile devices. These assets were managed to align with agency standards before network integration. 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 to determine 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. Further, DFC provided component authenticity/anti-counterfeit training for designated personnel and maintained configuration control over system components that are awaiting repair and service or repaired components awaiting return to service. Testing performed by the independent auditors found no exceptions for the SCRM program, and the controls were operating as intended. We determined 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 Managed and Measurable.

DFC consistently implemented an organization-wide configuration management plan, and the plan was integrated into risk management and continuous monitoring processes. DFC's Configuration Management Plan defined roles and responsibilities, initiated a Change Control Board, and outlined processes for identifying, managing, monitoring, and reporting configuration management activities. DFC monitored, analyzed, and reported qualitative and quantitative performance measures on the effectiveness of its change control activities and documented lessons learned on the effectiveness of its change control activities. In addition, DFC utilized various automated mechanisms to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact. Further, DFC remediated 97% of critical and high vulnerabilities within 30 days and successfully addressed a prior year issue regarding not timely remediated critical and high vulnerabilities. Hence, we determined FY 2023-Recommendation 1 is closed.[16] Testing performed by the independent auditors found no exceptions for the Configuration Management program, and the controls were operating as intended. We determined DFC's Configuration Management controls in place were overall effective.

Identity and Access Management

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

[16] FY 2023 FISMA Audit Report A-DFC-24-001-C

DFC ensured all personnel were assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. All remote access to DFC information systems was supported by the General Support System, which provided remote access service. DFC implemented a third-party identity management cloud service for its enterprise-wide single sign-on solution. All of the organization's systems interface with the solution to oversee employees, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis. 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 utilized lessons learned, end users' devices were properly configured, and privileged users utilized a strong authentication mechanism. Testing performed by the independent auditors found no exceptions for the Identity and Access Management program, and the controls were operating as intended. We determined 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. Further, DFC participated in a privacy breach tabletop exercise and used lessons learned to improve the Data Breach Response Plan as appropriate. Privacy awareness training was provided annually, and targeted phishing exercises were conducted for those responsible for PII. 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 overall effective.

Security Training

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

DFC performed roles and responsibilities for security training, completed workforce assessment, and annual security training. In addition, DFC addressed the knowledge, skills, and abilities gaps identified through talent acquisition. DFC also measured its awareness program's effectiveness by conducting phishing exercises and following up with additional awareness training and disciplinary action. DFC monitored and analyzed qualitative and quantitative performance measures to determine the effectiveness of its security awareness, training strategies, and plans, and training feedback was obtained accordingly. 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

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

DFC regularly analyzed performance metrics to adjust and improve its program. DFC transitioned to ongoing control and system authorization by implementing its continuous monitoring policies and strategy. In addition, DFC documented and implemented lessons learned to enhance the continuous monitoring process to instruct 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. Further, DFC implemented its system-level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans and monitoring security controls. DFC utilized Cybersecurity Security Assessment and Management (CSAM) as a monitoring mechanism to ensure the timely review and approval of system-level system security plans. Hence, we determined FY 2023-Recommendation 2 is closed.[17] Testing performed by the independent auditors found no exceptions for the ISCM program, and the controls were operating as intended. We determined 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. We found one weakness in the incident response domain regarding not reaching the event logging (EL) level 3 in accordance with OMB M-21-31.

DFC Must Fully Implement Event Logging Requirements Set Forth by OMB M-21-31

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, provides guidance for improving the federal government's cybersecurity posture through enhanced logging practices. The purpose of this memorandum is to focus on ensuring centralized access and visibility for each agency's highest-level enterprise security operations center. Agencies must retain, manage, and share their logs with the CISA and the Federal Bureau of Investigations (FBI) to defend federal information systems and assist third parties in detecting, investigating, and mitigating cyber threats in a timely manner. Failure to communicate security incidents to third parties during the audit log reporting process could allow attackers to cause damage and result in severe breaches. The memorandum states:

[17] FY 2023 FISMA Audit Report A-DFC-24-001-C

Section I: Maturity Model for Event Log Management

Tier EL1, Rating – Basic

The agency and all of its components meet the following requirements, as detailed in Table 2 (EL1 Basic Requirements) within Appendix A (Implementation and Centralized Access Requirements):

- Basic Logging Categories
- Minimum Logging Data
- Time Standard
- Event Forwarding
- Protecting and Validating Log Information
- Passive DNS [Domain Name System]
- Cybersecurity Infrastructure Security Agency (CISA) and Federal Bureau of Investigations (FBI) Access Requirements
- Logging Orchestration, Automation, and Response – Planning
- User Behavior Monitoring – Planning
- Basic Centralized Access

Tier EL2, Rating – Intermediate

The agency and all of its components meet the following requirements, as detailed in Table 3 (EL2 Intermediate Requirements) within Appendix A (Implementation and Centralized Access Requirements):

- Meeting EL1 maturity level
- Intermediate Logging Categories
- Publication of Standardized Log Structure
- Inspection of Encrypted Data
- Intermediate Centralized Access

Tier EL3, Rating – Advanced

The agency and all its components meet the following requirements, as detailed in Table 4 (EL3 Advanced Requirements) within Appendix A (Implementation and Centralized Access)

- Meeting EL2 maturity level
- Advanced Logging Categories
- Logging Orchestration, Automation, and Response – Finalizing Implementation
- User Behavior Monitoring – Finalizing Implementation
- Application Container Security, Operations, and Management
- Advanced Centralized Access

> Section II: Agency Implementation Requirements
>
> Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:
>
> - Within 18 months of the date of this memorandum, achieve EL2 maturity.
> - Within two years of the date of this memorandum, achieve EL3 maturity.

DFC did not implement event logging requirements to meet the EL2 (intermediate) or EL3 (advanced) level in accordance with the OMB memorandum M-21-31, dated August 27, 2021. DFC was required to reach EL3 maturity by August 2023. As of July 1, 2024, or 35 months since issuance, DFC was at maturity EL1 (basic) level. Specifically, DFC did not meet the audit logs at application levels, in which management stated that these applications are software as a Service (SaaS) and considered minor, with only selected users having access. Consequently, DFC would not be able to comply with the CISA and the FBI access requirements if such a request arises during a security compromise.

DFC's cloud service provider did not provide audit logs to DFC because their internal security protocols prevented them from sharing the audit log data with third parties. DFC had automated Continuous Diagnostics and Mitigation reporting of the agency logs, searching for evidence, and mitigating a potential or confirmed intrusion into DFC's network; however, the application logs were missing. DFC officials stated that DFC relies on the Federal Risk and Authorization Management Program SaaS to capture the application logs. DFC was in the process of addressing the logging gap and expected complete onboarding of its systems through the [redacted] into a third-party provider within the next three months.

For SaaS products that lack the capability for individualized export of customer audit logs, attackers may be able to cause damage, and potential threats or breaches might go unnoticed because security incidents were not communicated to third parties during the audit log reporting process. Effective incident response relies on detailed logs to understand the nature and scope of an incident, so deficient logging can hinder the ability to respond promptly and appropriately. Logs are essential for forensic analysis to determine how an attack occurred, what was affected, and how to prevent future incidents; inadequate logs can severely limit the effectiveness of such analyses.

> **Recommendation 1**: We recommend that DFC's Chief Information Officer fully implement event logging requirements in accordance with Office of Management and Budget, Memorandum M-21-31.

Although the DFC did not reach the EL3 level by August 2023 per the requirement of OMB M-21-31, 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. As a result, the DFC could be assembled quickly to meet the required reporting timelines and expedite reporting of incidents. Additionally, we noted that DFC used several software tools to detect suspected incidences and utilized dashboards to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures, and ensured that data supporting metrics were obtained accurately and consistently, and in a reproducible format. Further, DFC utilized profiling techniques to maintain a comprehensive baseline of network operations. Our overall control testing 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 Incident Response controls in place were overall effective.

Contingency Planning

We determined the DFC's overall maturity level for the Contingency Planning program was Managed and Measurable. We found one weakness in the contingency planning domain regarding reviewing and authorizing the COOP and integrated metrics on the effectiveness of its information system contingency plans with the COOP.

DFC Must Review and Approve its COOP

According to OPIC's Continuity Plan, April 2016, page viii, the OPIC Continuity Plan is reviewed and updated annually. If changes are made to the continuity plan outside the official cycle of plan review, coordination, and update, planners will track and record the changes using the record of changes below.

In addition, the NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, page 9, states, "COOP planning applies to mission essential functions of federal government departments and agencies. ISCPs [Information System Contingency Plans] apply to all information systems in federal organizations. AUTHORITIES: COOP is mandated for federal organizations by HSPD-20 [Homeland Security Presidential Directive-20] / NSPD-51 [National Security Presidential Directive-51], FCDs [Federal Continuity Directives] 1 and 2, and the National Continuity Policy Implementation Plan (NCPIP); ISCPs are mandated for federal organizations by FISMA." Furthermore, *Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements,* required continuity programs must address all elements of continuity: program management, plans, and procedures; essential functions; orders of succession; delegations of authority; communications and information systems; essential records management; alternate locations; human resources; devolution; reconstitution; test, training, and exercises; and, the four phases of continuity: (1) readiness and preparedness, (2) activation, (3) continuity operations, and (4) reconstitution. It also requires a review of the organization's continuity plan annually and an update as required. The date of the review and the names of personnel conducting the review must be recorded.

RMA found that DFC did not integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related business process continuity plan to deliver persistent situational awareness across the organization. During the audit, the current draft of the COOP is pending review and approval. As such, the COOP plan was not tested for effectiveness. The last approved version of the COOP was in 2016.

DFC did not have an adequate monitoring mechanism to ensure the timely review, approval, and testing of the COOP's effectiveness. Without consistently reviewing and authorizing the COOP, DFC may not be able to ensure that the agency is able to continue the performance of essential functions during a wide range of emergencies.

RMA does not issue a new recommendation for this finding in the FY 2024 FISMA Audit because this issue was reported as a management letter comment during the FY 2023 DFC Financial Statement Audit, and an open item is pending addressing by management:

> FY 2023 DFC Financial Statement Audit (23-03): *RMA recommends that the DFC Vice President and Chief Administrative Officer implement the necessary oversight to ensure that the Continuity of Operations Plan is reviewed and authorized annually in accordance with the timeliness requirements defined by DFC.*

Although the COOP was still in draft and had not been tested for effectiveness and integrated with information contingency plans, 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. Further, DFC ensured that the data supporting the metrics were obtained accurately, consistently, and in a reproducible format. Our overall control testing 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 Contingency Planning controls were overall 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 Domains. We determined the DFC's information security program and practices were effective for FY 2024, 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 incident response and contingency planning domains. We made one recommendation to assist DFC in strengthening its information security program. Further, all two prior FISMA performance audit recommendations were closed.

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 2024 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 2024 as of July 31, 2024. We assessed four internal and external systems out of four FISMA reportable systems from DFC's information system inventory. The performance audit fieldwork covered DFC's headquarters in Washington, DC, and audit work was conducted between February 1 and July 31, 2024. The performance audit included steps to follow up on deficiencies from the prior year.

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.

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 the effectiveness of the security controls relevant to the 20 core metric questions and 17 FY 2024 supplemental metric questions specified in OMB's *FY 2023 – 2024 IG FISMA Metrics*, we tested the entire DFC administrative controls population. The application controls were the responsibility of the DFC's service providers.

We focused our FY 2024 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 2024 FISMA audit:

NIST Federal Information Processing Standards (FIPS) 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 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5.1.1, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 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 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management*

OMB Policy Directives

- OMB Memorandum M-24-04, *Fiscal Year 2024 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-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Memorandum M-17-09, *Management of Federal High Value Assets*
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Circular A-123 - *Management's Responsibility for Internal Control*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

GAO

- Standards for Internal Control in the Federal Government (September 2014)

DHS

- *FY 2023 – 2024 IG FISMA Reporting Metrics*
- DHS Binding Operational Directive 23-01, *Implementation Guidance for Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- DHS Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- 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 Binding Operational Directive 18-02 *Securing High Value Assets*
- 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*
- 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 Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*

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
COOP	Continuity of Operations Plan
CSAM	Cybersecurity Security Assessment and Management
DFC	United States International Development Finance Corporation
DHS	Department of Homeland Security
DNS	Domain Name System
EL	Event logging
FBI	Federal Bureau of Investigations
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
ISCP	Information System Contingency Plan
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
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
SaaS	Software as a Service
SCRM	Supply Chain Risk Management
SP	Special Publication
TIC	Trusted Internet Connection

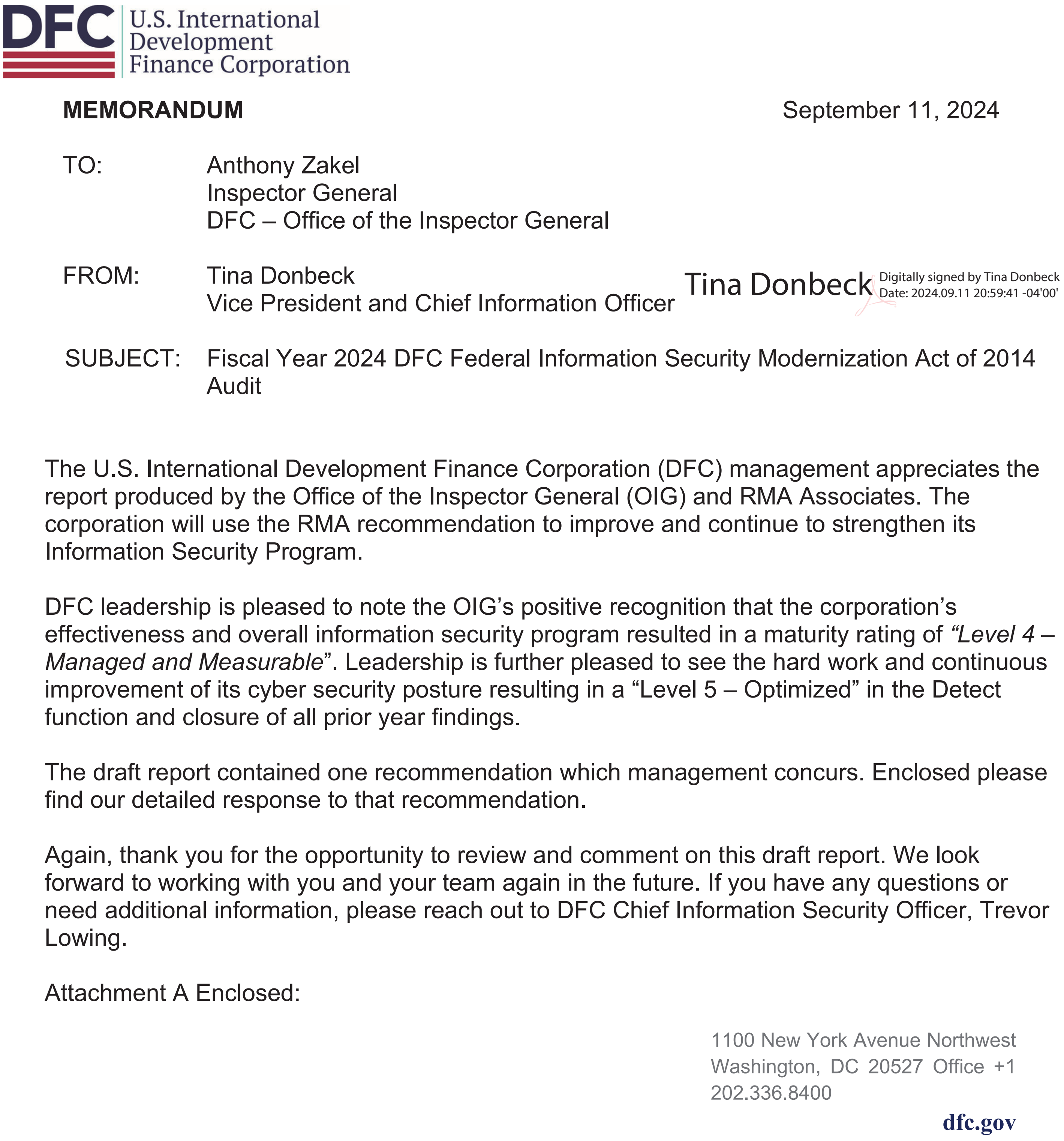
Appendix I: Status of Prior Year Recommendations

The following table provides the status of the FY 2023 FISMA performance audit recommendations.

Table 5: FY 2023 FISMA Performance Audit Recommendations

Recommendation No.	Audit Recommendations	DFC's Position	Auditor's Position on the Status
FY 2023 Audit Report A-DFC-24-001-C			
1	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.	Closed	Agree. Refer to Audit Results – Configuration Management domain
2	Implement the necessary oversight to monitor Cybersecurity Security Assessment and Management (CSAM) to ensure that System Security Plans are reviewed and authorized in accordance with the timeliness requirements in DFC's policy.	Closed	Agree. Refer to Audit Results – Information Security Continuous Monitoring domain

Appendix II: Management Response



DFC U.S. International Development Finance Corporation

MEMORANDUM September 11, 2024

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

FROM: Tina Donbeck
Vice President and Chief Information Officer

Tina Donbeck Digitally signed by Tina Donbeck
Date: 2024.09.11 20:59:41 -04'00'

SUBJECT: Fiscal Year 2024 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 recommendation to improve and continue to strengthen its Information Security Program.

DFC leadership is pleased to note the OIG's positive recognition that the corporation's effectiveness and overall information security program resulted in a maturity rating of *"Level 4 – Managed and Measurable*". Leadership is further pleased to see the hard work and continuous improvement of its cyber security posture resulting in a "Level 5 – Optimized" in the Detect function and closure of all prior year findings.

The draft report contained one recommendation which management concurs. Enclosed please find our detailed response to that recommendation.

Again, thank you for the opportunity to review and comment on this draft report. We look forward to working with you and your team again in the future. If you have any questions or need additional information, please reach out to DFC Chief Information Security Officer, Trevor Lowing.

Attachment A Enclosed:

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

dfc.gov

DFC U.S. International Development Finance Corporation

Attachment A: Response from the Office of Information Technology (OIT), Chief Information Officer regarding OIG Recommendation 1of Fiscal Year 2024 DFC Federal Information Security Modernization Act of 2014 Audit

Recommendation 1: We recommend that DFC's Chief Information Officer fully implement event logging requirements in accordance with Office of Management and Budget, Memorandum M-21-31.

Management Response: Concur

The CISO team will perform a comprehensive gap analysis in collaboration with [redacted] and DFC Infrastructure teams to identify and prioritize issues and systems of importance (FISMA Systems). This encompasses active engagement with external OIT teams managing SaaS systems to ensure clear communication and defined responsibilities.

A key element of our strategy is to evaluate systems lacking established logging protocols for integration into [redacted]. This requires the development, documentation, and execution of change management procedures for each system to facilitate log collection. The remediation efforts will concentrate on addressing the most critical gaps first (FISMA Systems), with a preference for direct logging via [redacted] or secure alternatives. The remediation progress will be closely monitored and consistently reported back to management. After remediation, the CISO team will verify compliance and establish regular checks to maintain adherence. The initial analysis phase of the project is slated to commence by the end of September, followed by further planning after the analysis is completed. The total remediation phase is anticipated to take up to 6 months, concluding by December 2025.

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

dfc.gov

Appendix III: Evaluation of Management Response

In response to the draft report, DFC's comments are included in **Appendix II: Management Response**. Management indicated that the target implementation date to address Fiscal Year (FY) 2024 - Recommendations 1 is December 2025.

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