OFFICE OF INSPECTOR GENERAL

U.S. International Development Finance Corporation

Fiscal Year 2022 DFC Federal Information Security Modernization Act of 2014 Audit

November 09, 2022

Audit Report DFC-23-001-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

DFC Implemented an Ineffective Information Security Program by Achieving an Overall Defined Maturity Level Based on the FY 2022 Core Inspector General FISMA Metrics

What We Reviewed

We 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) 2022 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 2022 Core Inspector General (IG) FISMA Metrics.* The *FY 2022 Core IG Metrics* classifies information security programs and practices into five (5) maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

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 2022 Core IG FISMA Metrics.*

What We Found

In its audit of DFC, RMA reported DFC's information security program and practices were ineffective for FY 2022, and the overall maturity level of the DFC's information security program was Defined.

Three (3) factors that drive the root cause of why DFC was downgraded from Managed and Measurable (effective) in FY 2021 to the Defined (ineffective) maturity level in FY 2022 include the following:

1. DFC did not execute the security practices required by the Office of Management and Budget (OMB) and U.S. Department of Homeland Security (DHS).
2. The decrease of 66 metrics in FY 2021 to 20 in FY 2022 affected the FISMA scoring methodology.
3. The time constraints in the FY 2022 FISMA audit period (OMB compressed the schedule to three (3) months sooner this year – IG FISMA Metrics reports are now due by July instead of October).

Our Recommendations

We made six recommendations to DFC that will further strengthen DFC's information security program. RMA recommends the Chief Information Officer:

- **Recommendation 1:** Update its Authorization to Operate and system-level Security Assessment Reports annually.
- **Recommendation 2:** Implement a plan to replace or upgrade the unsupported software within DFC's network.
- **Recommendation 3:** Document and implement 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.
- **Recommendation 4**: Perform the breach tabletop exercises annually.
- **Recommendation 5**: Develop a methodology and implement a tool to track the timely review of periodic updates for BIAs and contingency tests.
- **Recommendation 6**: Update DFC's Vulnerability and Risk Management Program to differentiate vulnerabilities remediation timeframe between internal and external facing systems and align with timeframes in the DHS's *FY 2022 Core IG FISMA Metrics*.

OFFICE OF INSPECTOR GENERAL

U.S. International Development Finance Corporation

Date: November 09, 2022

MEMORANDUM FOR: MS. TINA DONBECK
CHIEF INFORMATION OFFICER (CIO)

FROM: Anthony “Tony” Zakel
Inspector General

SUBJECT: Final Report – (Fiscal Year 2022 DFC Federal Information Security Modernization Act of 2014 Audit) (Report Number DFC-23-001-C)

Enclosed is the final report on Fiscal Year 2022 DFC Federal Information Security Modernization Act of 2014 Audit, which presents the results of our review. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of RMA Associates LLC to conduct the audit. The contract required the audit to be performed in accordance with 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).

RMA is responsible for the attached auditor's report dated November 09, 2022 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: Chief Executive Officer
Chief Operating Officer
Chief Risk Officer
All Vice Presidents
Director of Internal Controls
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

Audit Report for Fiscal Year 2022

RMA | Associates
Auditors. Consultants. Advisors.

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

September 26, 2022

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 2022

Dear Mr. Zakel:

RMA Associates, LLC is pleased to submit the United States International Development Finance Corporation (DFC) Federal Information Security Modernization Act of 2014 (FISMA) Audit Report for Fiscal Year (FY) 2022.

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 outlined in the *FY 2022 Core IG FISMA Metrics*. We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (also known as the Yellow Book) issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We have also prepared the answers to the Office of Management and Budget's (OMB) Fiscal Year 2022 Core Inspector General Metrics (April 2022). These metrics provide reporting requirements across functional areas to be addressed in the independent assessment of agencies' information security programs.

In summary, we found the DFC's information security program and practices were ineffective for FY 2022, and the overall maturity level of the DFC's information security program was Defined.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

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 United States International Development Finance Corporation's (DFC) information security program and practices for fiscal year (FY) 2022 in accordance with the *Federal Information Security Modernization Act of 2014* (FISMA). FISMA[1] 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.

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 outlined in the *FY 2022 Core IG FISMA Metrics.*

For this year's review, OMB required inspectors generals to assess 20 of the 66 metrics from *FY 2021 IG FISMA Reporting Metrics v1.1* (May 12, 2021). The FY 2022 Core Inspectors General (IG) Metrics were aligned with the five (5) following Cybersecurity Framework security functions areas: Identify, Protect, Detect, Respond, and Recover to determine the effectiveness of agencies' information security program. The FY 2022 Core IG Metrics classifies information security programs and practices into five (5) maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

The audit included an assessment of DFC's information security program and practices consistent with FISMA and reporting instructions issued by OMB. We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as specified in the most current version of the Government Accountability Office's Government Auditing Standards (GAO "Yellow Book" / GAGAS), as well as guidelines established by the OMB Department of Homeland Security (DHS), and National Institute of Standards and Technology (NIST) guidance. 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 audit objective. We believe that the evidence obtained provides a reasonable basis for determining the maturity level for the core metrics and conclusions based on our audit objective. We also assessed selected security controls outlined in *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of four (4) internal and external systems out of a total of four (4) FISMA reportable systems from DFC's FISMA inventory of information systems.

RMA conducted a FISMA audit for FY 2022 as of July 30, 2022. The audit fieldwork covered DFC's headquarters located in Washington, DC, from February 24 to September 23, 2022.

[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 concluded that DFC implemented an ineffective information security program by achieving an overall Defined maturity level based on the *FY 2022 Core IG FISMA Metrics*. Our tests of the information security program found six (6) significant control issues that fell in the risk management, data protection and privacy, information security and continuous monitoring, and contingency planning domains. In addition, we found one (1) observation that fell in the configuration management domain of the *FY 2022 Core FISMA Metrics*. We have made six (6) recommendations to assist DFC in strengthening its information security program. Further, we noted five (5) recommendations in prior FISMA 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. RMA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their status. The information included in this report was obtained from DFC on or before September 23, 2022. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 23, 2022.

Additional information on our findings and recommendations are included in the accompanying report. We are submitting this report to the United States International Development Finance Corporation Office of Inspector General.

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

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
FY 2022 Core IG Metrics 5
Summary Audit Results 6
Objective, Scope, and Methodology 15
Abbreviations 20
Appendix I - Status of Prior Year Findings 21
Appendix II: Management Response 23
Appendix III: Evaluation of Management Response 28

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

Introduction

This report presents the results of our 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 Office of Inspector General (OIG) engaged RMA Associates, LLC (RMA) to conduct an annual audit of the DFC's information security program and practices in support of the FISMA audit requirement. 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 outlined in the *FY 2022 Core Inspectors General (IG) FISMA Metrics*.

As part of our audit, we responded to the FY 2022 Core Inspector General Metrics (FY22 Core IG Metrics) specified in OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines.*[3] These core metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs. See *Objective, Scope, and Methodology* for more details. We also considered applicable OMB policy and guidelines, and the NIST standards and guidelines.

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

[2] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).
[3] Per OMB Memorandum M-22-05, the timeline for the IG audit of agency effectiveness was adjusted to align the results of the audit with the budget submission cycle. Representatives from OMB, Federal Civilian Executive Branch Chief Information Security Officer teams, CIGIE, and the Intelligence Community agreed that the 20 Core IG Metrics should provide sufficient data to determine the effectiveness of an Agency's information security program with a high level of confidence.

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

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 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 Federal 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.

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

NIST developed an integrated Risk Management Framework that effectively combines all the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

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

Key Changes to the Metrics

One of the annual FISMA audit goals is to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. The OMB Office of the Federal Chief Information Officer published Core Metrics, which is geared to the President's agenda, on April 13, 2021. The OMB issued Memorandum M-22-05[4], which provides guidance on Federal Information Security and Privacy Management Requirements. The metrics are based on coordinated discussions between (and the consensus opinion of) representatives from OMB, CIGIE, Federal Civilian Executive Branch Chief Information Security Officers and its staff, and the Intelligence Community. Research, interviews, and IG survey data provided quantitative and qualitative information to formulate these guidelines. The core metrics consist of 20 of the 66 FISMA questions from *FY 2021 IG FISMA Reporting Metrics v1.1* (May 12, 2021). The FY 2022 Core IG Metrics were chosen based on alignment with Executive Order (EO) 14028 (May 12, 2021), *Improving the Nation's Cybersecurity,* as well as recent OMB guidance to agencies in furtherance of the modernization of Federal cybersecurity, including:

- *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (M-22-09) – OMB and Cybersecurity & Infrastructure Security Agency (CISA) solicited public feedback on strategic and technical guidance documents meant to move the U.S. government towards a zero-trust architecture. OMB's Federal Zero Trust Strategy aims to accelerate agencies towards a baseline of early zero trust maturity.
- Multifactor Authentication (MFA) and Encryption (EO 14028) – Per the EO, agencies were required to fully adopt MFA and encryption for data at rest and in transit by November 8, 2021. For agencies that were unable to meet these requirements within 180 days of the date of the order, the agency head was directed to provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the Assistant to the President and National Security Advisor.
- *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31) – This memorandum provides specific requirements for log management. It includes a maturation model, prioritizing the most critical log types and requirements, to build a roadmap to success.
- *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01) – On October 8, 2021, this memorandum was issued for agencies to focus on improving early detection capabilities, creating "enterprise-level visibility" across components and sub-agencies, and requires agencies to deploy an Endpoint Detection and Response solution.
- Software Supply Chain Security & Critical Software – Section 4 of EO 14028 tasks OMB, NIST, and other Federal entities with developing new guidelines and frameworks to improve the security and integrity of the technology supply chain. In collaboration with

[4] M-22-05 *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, December 6, 2021.

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

industry and other partners, this effort provides frameworks and guidelines on how to assess and build secure technology, including open-source software.

Additionally, OMB Memorandum M-22-05 adjusts the timeline for the IG audit of agency effectiveness to align the results of the audit with the budget submission cycle. Historically, the audit of agency effectiveness by IGs finished in October. However, for FY 2022 the IG audit completion (submission to the Cyber Scope system) deadline has shifted from October to July to better align the release of IG assessments with the development of the President's Budget as mentioned in OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*. The previous timeline limited agency leadership's ability to request resources in the next Budget Year submissions to provide for remediations. The expectation is this change will reduce the time between issue identification, resource request, and allocation.

FY 2022 Core IG Metrics

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 2022 Core IG Metrics classifies information security programs and practices into five (5) 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

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 on 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.

Our audit was conducted for FY 2022 as of July 30, 2022. It consisted of testing the 20 core metric questions listed in the FY 2022 Core IG Metrics issued by OMB. The FY 2022 Core IG Metrics were aligned with the five (5) Cybersecurity Framework security functions areas (key performance areas) as follows:

- Identify, which includes questions pertaining to Risk Management and Supply Chain Risk Management (SCRM);

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

- 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.

Summary Audit Results

We concluded 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 (5) Cybersecurity Functions[5] and nine (9) FISMA Metric Domains.[6] The overall maturity level of the DFC's information security program was determined as Defined, as described in this report. Accordingly, we found the DFC's information security program and practices were ineffective for FY 2022.

We provided the DFC with a draft of this report for comment. In a written response, management agreed with the results of our audit. See *Management Response* in Appendix II for the DFC's response in its entirety.

We determined the maturity level for each FISMA domain based on the responses to the 20 questions in the FY 2022 Core IG Metrics and testing for each domain. The overall maturity level of the DFC's information security program was determined as Defined based upon a majority of the component scores for each domain's maturity level. Our tests of the information security program found six (6) significant control issues, and one (1) observation, which concluded the DFC's security program controls in place were ineffective.

We have presented the maturity level for the nine (9) domains below:

Table 2: The DFC's FY 2022 Maturity Levels

Function	Maturity Level	
Function 1: Identify		Defined (Level 2)
• Risk Management	Defined (Level 2)	
• Supply Chain Risk Management	Defined (Level 2)	
Function 2: Protect		Optimized (Level 5)

[5] 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*.

[6] 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

Function	Maturity Level	
• Configuration Management	Optimized (Level 5)	
• Identity Management	Optimized (Level 5)	
• Data Protection and Privacy	Managed and Measurable (Level 4)	
• Security Training	Defined (Level 2)	
Function 3: Detect—Information Security Continuous Monitoring		Defined (Level 2)
Function 4: Respond—Incident Response		Optimized (Level 5)
Function 5: Recover—Contingency Planning		Defined (Level 2)
	Overall	**Defined (Level 2)**
	Overall	**Ineffective**

Below is the maturity level for each domain.

Risk Management

We determined the DFC's overall maturity level for the Risk Management program was Defined.

DFC Needs to Perform Ongoing Security Control Assessments

RMA found that DFC did not follow NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* to assess the controls in the system and its environment of operation (CA-2 Control Assessment) and authorize the system to operate (CA-6 Authorization). Specifically, DFC did not consistently update its Authorization to Operate (ATOs) and system-level Security Assessment Reports (SARs) for the four (4) selected systems. The lack of current ATOs increases the risk of maintaining systems and data confidentiality, integrity, and availability. The delay in conducting security assessment and authorization minimizes the agency's effectiveness in monitoring risk and ensuring security controls are working as intended.

> **Recommendation 1**: RMA recommends that the Chief Information Officer update its Authorization to Operate and system-level Security Assessment Reports annually.

DFC Needs to Remove Unsupported Software and Remediate Known Exploited Vulnerabilities Within DFC's Defined Remediation Timeframe

According to NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* an agency is required to replace system components when support for the components is no longer available from the developer, vendor, or manufacturer (SA-22 Unsupported System Components). Additionally, NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Technologies* states that "installing a patch or update or upgrading software to a newer version without the vulnerabilities are the only forms of risk response that can completely eliminate the vulnerabilities without removing functionality." RMA found that DFC's software inventory included unsupported software resulting in four (4) outstanding known exploited vulnerabilities identified on the vulnerability scans, and 24 of the 56 high-risk

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

vulnerabilities were identified prior to January 2022 and had not been remediated by June 2, 2022. Approximately 43 percent of those high vulnerabilities were over 45 days old. DFC did not remediate its vulnerabilities in accordance with the timeframes in DFC's Vulnerability Patch Compliance policy. Hence, RMA determined FY 2018-Recommendation 2 and 3[7], and FY 2017 Recommendation 1[8] remain open and is not making a new recommendation.

This issue also resulted in last year's FISMA audit report[9] and DFC had documented Risk Acceptance memo and compensating controls regarding the unsupported software known exploited vulnerabilities. However, RMA found that DFC did not have an effective process for removing unsupported software from its devices in a timely manner. Software that is no longer supported by vendors was in use and exposed the DFC to vulnerabilities that are difficult to mitigate effectively. The use of unsupported software increases the risk that known exploitable vulnerabilities will be exploited. Effective vulnerability management reduces the risk of successful harmful breaches and decreases the time and effort necessary to respond after a breach appropriately. Hence, RMA determined FY 2021-Recommendation 1[10] is closed and is making a new recommendation to address the unsupported software issue specifically.

> **Recommendation 2**: RMA recommends that the Chief Information Officer implement a plan to replace or upgrade the unsupported software within DFC's network.

DFC Needs to Develop a Process to Document and Implement Risk Management Lessons Learned

According to NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations A System Lifecycle Approach for Security and Privacy*, an agency is required to incorporate lessons learned as continuous monitoring and ongoing authorization processes are implemented for moderate impact and high impact systems. RMA found that DFC lacks a formal, prescriptive lesson learned process for its Risk Management process. Without a formal, disciplined lesson learned process, DFC may not capture information from previous updates and from actual risk events, which may cause DFC to miss the opportunities to strengthen its security posture.

> **Recommendation 3**: RMA recommends that the Chief Information Officer document and implement 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.

After the audit fieldwork, DFC updated its *DFC Continuous Monitoring Plan,* which documents the requirement to conduct lessons learned during its control assessment. However, the FY 2022-

[7] FY 2018 FISMA Audit Report A-OPC-19-006-C
[8] FY 2017 FISMA Audit Report A-OPC-17-007-C
[9] FY 2021 FISMA Audit Report A-DFC-22-003-C
[10] Ibid

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

Recommendation 3 will remain open until RMA verifies the implementation of lesson-learned requirements as defined in the *Continuous Monitoring Plan* in the FY 2023 FISMA Audit.

Supply Chain Risk Management

We determined the DFC's overall maturity level for the SCRM program was Defined.

RMA found that the DFC had made improvements to develop the Supply Chain policies and procedures. In addition, DFC established a work intake process that formalizes Information Technology (IT) software requests and developed an SCRM checklist in June 2022; however, DFC indicated that they did not have an instance of new software that required the use of the checklist since implementation. The work intake process was not used for evaluating current software or software relicensing. As such, we determined DFC did not consistently implement a process for assessing, through an audit, test results, and other forms of evaluation of DFC's supply chain-related risks and did not use qualitative and quantitative performance metrics to measure and report on SCRM products, systems, and services. Hence, RMA determined FY 2021-Recommendation 3[11] remains open and is not making a new recommendation.

Configuration Management

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

DFC consistently tested for both code-based and configuration-based vulnerabilities through utilizing its SCAP-validated software scanning tools on all systems and has formally documented lessons learned to improve its secure configuration policies and procedures. DFC employed automation tools to help maintain an up-to-date, accurate, and readily available view of the security configurations for all information system components connected to its network and make appropriate modifications and deployed system configuration management tools that automatically enforce and redeploy configuration settings to systems. RMA determined that controls were operating as intended. We concluded the DFC's Configuration Management program controls in place were effective.

Identity and Access Management

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

All remote access to DFC information systems was supported via the DFCNet-provided remote access service. DFC implemented Okta as an 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 in a near real-time basis. DFC's implementation of its Single Sign-On Solution Okta, together with

[11] Ibid

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

its integration with Active Directory, demonstrates that DFC employs automated mechanisms to manage privileged accounts, including the automatic removal of temporary, emergency, and inactive accounts. However, RMA found that DFC's MFA was not enforced on servers for administrators as DFC used password login for servers for its admin personnel. Hence, RMA determined FY 2020-Recommendation 3[12] remains open and is not making a new recommendation. Although our testing found one (1) exception; however, it was a known issue, and the controls were operating as intended. We concluded the DFC's Identity and Access Management program controls in place were 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 Needs to Conduct Data Exfiltration/Table-Top Exercises for FY 2022

According to the OMB M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information*, an agency is required to periodically, but not less than annually, hold a tabletop exercise to test the breach response plan and to help ensure that members of the team are familiar with the plan and understand its specific roles. RMA found that DFC did not conduct data exfiltration/tabletop exercises for FY 2022. By not performing a tabletop/data exfiltration exercise for the data breach, DFC may not be prepared to react to a data breach, and there is an increased risk confidentiality, integrity, and availability of information may be comprised.

> **Recommendation 4**: RMA recommends that the Chief Information Officer perform the breach tabletop exercises annually.

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, the 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. RMA inspected the Device Encryption report from the Endpoint Management Software utilized by DFC and determined that DFC encrypts its laptops. We also determined that every laptop was fully encrypted. Hence, RMA determined FY 2021-Recommendation 2[13] is closed. Although we found an exception that DFC did not conduct data exfiltration/tabletop exercise for FY 2022; however, management stated that prior lessons learned were considered as part of the incident review process. Our control testing determined that the controls were operating as intended. We concluded the DFC's Data Protection and Privacy program controls were effective.

[12] FY 2020 FISMA Audit Report A-DFC-21-005-C
[13] 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

After audit fieldwork, DFC conducted the Data Exfiltration Exercise on September 12, 2022 to test the DFC's ability to detect the exfiltration or attempted exfiltration of sensitive data. As such, RMA determined that FY 2022-Recommendation 4 is closed.

Security Training

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

RMA found that DFC had made improvements in its policies to define its processes for assessing the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment; however, the policies and procedures, Information Security Program Plan (ISPP), are pending management approval and in draft status since May 2020. In addition, we noted that DFC assessed workforce gaps and vacancies and was able to fill the identified workforce gaps with new hires for the FY 2021-FY 2022 period. However, we found that DFC's assessment did not include a comprehensive review of workforce skills and IT expertise. Although the maturity level of this domain was Defined, our control testing for this domain found the controls were operating as intended. We concluded the DFC's Security Training program controls in place were ineffective. We did not make a recommendation; however, we verbally informed management that the policies and procedures must be finalized and a comprehensive review of workforce skills and IT expertise must be performed to reach the Managed and Measurable level in the future.

Information Security and Continuous Monitoring

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

DFC Needs to Perform Ongoing Security Control Assessments

According to NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, an agency is required to assess the controls in the system and its environment of operation (CA-2 Control Assessment) and perform ongoing control assessments in accordance with the continuous monitoring strategy (CA-7 Continuous Monitoring). DFC's policies and NIST's guidance require a system to undergo an assessment before it is connected to the DFC network. RMA found that DFC did not consistently perform a continuous assessment of controls for the four (4) selected systems according to its ISCM policy. These systems operate without valid authorization. DFC does not know whether the security controls are operating as intended. Over time, security controls may change due to new technologies, changing security requirements, and a lack of personnel following security procedures which increases the risk of the confidentially, integrity, and availability of DFC's information and systems.

Recommendation: Refer to FY 2022 – Recommendation 1

DFC Needs to Develop a Process to Document and Implement ISCM Lessons Learned

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

According to NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations A System Lifecycle Approach for Security and Privacy*, an agency is required to incorporate lessons learned as continuous monitoring and ongoing authorization processes are implemented for moderate impact and high-impact systems. RMA found that DFC did not have a formal process to document and implement ISCM lessons learned to improve its existing controls' effectiveness. Without a formal, disciplined lesson learned process, DFC may not capture information from previous practice and from actual risk events, which may cause DFC to lose the opportunity of strengthening its security posture.

Recommendation: Refer to FY 2022 – Recommendation 3

Incident Response

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

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. As a result, the DFC could be assembled quickly to meet the required reporting timelines and expedite reporting of incidents. Additionally, RMA 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, consistently, and in a reproducible format. Our overall control testing for this domain found no exceptions, and the controls were operating as intended. We concluded 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 Defined.

DFC Needs to Consistently Review and Authorize Its Business Impact Analysis (BIA)

According to NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, the agency must identify the essential mission, business functions, and associated contingency requirements. Additionally, DFC's *Office of Information Technology (OIT) Contingency Plan Procedures*, Version 2.0 defined that a contingency plan shall be developed in accordance with NIST SP 800-34, current Business Impact Assessments, and with input from the Continuity of Operations Plan (COOP) coordinator. RMA found that DFC did not approve and authorize its BIA for one (1) of the four (4) systems selected for testing. RMA found that the BIA was in draft status since June 2021. DFC stated that they were in the process of migrating the active directory, domain users, data, and applications from OPIC to DFC for DFCNet and made a

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

decision to wait to complete the BIA until the migration was completed. The BIA assessment[14] was not completed prior to this migration since many of its systems configurations were changing. As a result, it would change the business impact and require a reassessment and reapproval. Outdated or inaccurate BIAs increase the risk that the agency would be unable to prioritize recovery operations effectively in the event of a service-impacting incident.

> **Recommendation 5**: RMA recommends that the Chief Information Officer develop a methodology and implement a tool to track the timely review of periodic updates for BIAs and contingency tests.

DFC Needs to Consistently Test Its System Contingency Plans

According to DFC's *Office of Information Technology (OIT) Contingency Plan Procedures*, Version 2.0, DFC defined that System Owners shall ensure that contingency plans for systems are tested/exercised at least annually in compliance with NIST SP 800-34. However, RMA found that two (2) cloud systems contingency plans were not tested within the past year. Testing system contingency plans is critical to ensuring effective system contingency plans are in place. Without effective system contingency plans, DFC's mission data is at a higher risk of loss due to an unscheduled disruption. Specifically, unscheduled disruptions in operations may debilitate the DFC, such that it may be unable to recover and continue operations of all necessary systems and functions in a timely manner.

> **Recommendation**: Refer to FY 2022 – Recommendation 5

Other Observation

DFC Needs to Revise Its Policies and Procedures Regarding Vulnerability Remediation Timeframes Based on the DHS FISMA Guidance

The FY 2022 Core IG FISMA Metrics (April 2022), Question 21, requires the agency patches critical vulnerabilities within 30 days to meet the Consistently Implemented level. RMA found that DFC did not document its process to patch critical vulnerabilities within 30 days. Additionally, DFC's Vulnerability and Risk Management Program (December 2021) did not differentiate between internal and external facing systems. It states Critical/High vulnerabilities need to be remediated, mitigated, or accepted within 45 days of being identified by Nessus Tenable (based on plugin modification date), Office of Chief Information Security Officer (OCISO), or issued by the DHS CISA. DFC did not have any vulnerabilities that resulted in external scans conducted by CISA. However, to reach Consistently Implemented, DFC needs to document the patching process to remediate the vulnerabilities within 30 days as required by the DHS. Without remediating vulnerabilities in a timely manner, DFC exposes its network to cyberattacks and leaves data susceptible to unauthorized disclosure and modification.

[14] On May 19, 2022, DFC presented an approved BIA and informed that the Information System Contingency Plan (ISCP) is also in the process of being finalized since the domain migration is now 90% completed.

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

Recommendation 6: RMA recommends that the Chief Information Officer update DFC's Vulnerability and Risk Management Program to differentiate vulnerabilities remediation timeframe between internal and external facing systems and align with timeframes in the Department of Homeland Security's Fiscal Year 2022 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.

After audit fieldwork, DFC modified its *Vulnerability and Risk Management Policy* with the timeframes aligning with DHS guidance. DFC also specified and differentiated vulnerability remediation timeframe between internal and external facing systems. As such, RMA determined that FY 2022-Recommendation 6 is closed.

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we concluded that the DFC's information security program and practices were established. They had been maintained for the five (5) Cybersecurity Functions and nine (9) FISMA Metric Domains. We found the DFC's information security program and practices were ineffective for FY 2022, and the overall maturity level of the DFC's information security program was Defined.

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 United States International Development Finance Corporation (DFC) achieved for each of the core metrics outlined in the *Fiscal Year (FY) 2022 Core IG FISMA Metrics.* Specifically, the audit determined whether DFC implemented an effective information security program by evaluating the five (5) Cybersecurity Framework security functions as divided among nine (9) 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 audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of the FISMA audit work conducted by RMA was DFC agency wide and the time period reviewed was for FY 2022 as of July 30, 2022. RMA assessed four (4) internal and external systems out of a total of four (4) FISMA reportable systems from DFC's information system inventory. The audit fieldwork covered DFC's headquarters located in Washington, DC, and audit work was conducted between February 24 to September 23, 2022. The audit included steps to follow up on prior year deficiencies.

Methodology

The overall strategy of our audit considered the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* the FISMA Reporting Metrics from Council of the Inspectors General on Integrity and Efficiency (CIGIE), Office of Management and Budget (OMB), and Department of Homeland Security (DHS), and the DFC's policies and procedures. Our

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

testing procedures were developed from NIST SP 800-53A, Revision 5. We determined the overall maturity level of each of the nine (9) domains by a simple majority of the component scores of the maturity level of each question within the domain, in accordance with the FY 2022 Core IG Metrics. For each of the FISMA questions, we indicated whether the DFC achieved each maturity level by stating "MET" or "NOT MET."

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 specified in OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*[15], 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 2022 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 2022 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*

[15] Per OMB Memorandum M-22-05, the timeline for the IG audit of agency effectiveness was adjusted to align the results of the audit with the budget submission cycle. Representatives from OMB, Federal Civilian Executive Branch Chief Information Security Officer teams, CIGIE, and the Intelligence Community agreed that the 20 Core IG Metrics should provide sufficient data to determine the effectiveness of an Agency's information security program with a high level of confidence.

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

- 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*
- 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 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 (ERM)*

OMB Policy Directives

- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*
- 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*

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

- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High-Value Asset Program*
- OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Memorandum M-17-09, *Management of Federal High-Value Assets*
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CISP) for the Federal Civilian Government*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*
- OMB *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*

DHS Directives and Other Guidance

- 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*
- 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*

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

- 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

ATO	Authorization to Operate
BIA	Business Impact Analysis
BUILD Act	Better Utilization of Investments Leading to Development Act of 2018
CA	Security Assessment and Authorization
CIO	Chief Information Officer
CSIP	Cybersecurity Strategy and Implementation Plan
CISA	Cybersecurity and Infrastructure Security Agency
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CM	Configuration Management
COOP	Continuity of Operations Plan
CP	Contingency Planning
DCA	Development Credit Authority
DFC	United States International Development Finance Corporation
DHS	Department of Homeland Security
DNS	Domain Name System
EO	Executive Order
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Planning
ISPP	Information Security Program Plan
IT	Information Technology
NIST	National Institute of Standards and Technology
MFA	Multifactor Authentication
OCISO	Office of Chief Information Security Officer
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
SA	System and Service Acquisition
SAR	Security Assessment Reports
SCRM	Supply Chain Risk Management
SP	Special Publication
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 Findings

The following table provides the status of the FY 2021, FY 2020, FY 2018, & FY2017 FISMA audit recommendations.

Table 3: FY 2021, 2020, 2018 & 2017 FISMA Audit Recommendations

Recommendation No.	Audit Recommendations	DFC's Position	Auditor's Position on the Status
FY 2021 Audit Report A-DFC-22-003-C			
1	Develop and implement a process to include compensating controls to mitigate risk when accepting the risk of known vulnerabilities.	Closed	Agree. Refer to Audit Results – Risk Management domain
2	Document and implement a process to verify that laptops are encrypted and remediate instances of nonencrypted laptops.	Closed	Agree. Refer to Audit Results – Data Protection and Privacy domain
3	Document and implement a strategy, policy, and procedures to manage supply chain risks with suppliers, contractors and systems.	Closed	Disagree. Refer to Audit Results – SCRM domain
FY 2020 Audit Report A-DFC-21-005-C			
3	Implement multifactor authentication for network access for privileged accounts.	Open	Agree. Refer to Audit Results – Identity and Access Management domain
FY 2018 Audit Report A-OPC-19-006-C			
2	Remediate patch and configuration vulnerabilities in the network identified by the Office of Inspector General, as appropriate, and document the results or document acceptance of the risks of those vulnerabilities.	Open	Agree. Refer to Audit Results – Risk Management domain
3	Document and implement a process to verify that patches are applied in a timely manner.	Open	Agree. Refer to Audit Results – Risk Management domain
FY 2017 Audit Report A-OPC-17-007-C			
1	Remediate network vulnerabilities identified by the Office of Inspector General's contractor, as appropriate, or document acceptance of the risks of those vulnerabilities.	Open	Agree. Refer to Audit Results – Risk

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
			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 October 24, 2022

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

FROM: Tina Donbeck
Vice President & Chief Information Officer

SUBJECT: Fiscal Year 2022 DFC Federal Information Security Modernization Act of 2014 Audit

The U.S. International Development Finance Corporation (DFC) response to the recommendations made by the DFC Office of Inspector General (OIG) in the draft report titled *Fiscal Year 2022 DFC Federal Information Security Modernization Act of 2014 Audit* is provided below.

Implementing the BUILD Act and creating DFC from two legacy agencies was a significant undertaking from a convergence of technologies perspective and the insights from the FISMA audit are valuable as the agency continues to grow and update its supporting infrastructure. Over the past two years, OIT has been investing its resources to upgrade legacy IT architecture to support DFC's expanded mission, building renovations, personnel growth, and support for hybrid technologies - all while keeping day to day operations running smoothly and securely. This coincided with executing new cyber security directives and executive orders while also building a larger federal IT team to meet the agency's growing needs. With this tremendous time of growth coupled with OIT's ongoing response to remote work stemming from the COVID pandemic, this year's FISMA audit coincided with various circumstances impacting the maturity of DFC's information security program:

- The Fiscal Year (FY) 21 FISMA audit ended December 2021 and the FY 22 FISMA audit kicked off February 2022. With only two months between audits due to changed OMB audit timelines, DFC was constrained to perform corrective actions needed from prior years audit due to compressed time and resources availability.

- The FY 22 Continuing Resolution was not lifted until March 2022. This impacted OIT's ability to get IT tools and contractor resources onboard to perform corrective actions on previously planned timelines.

- With the lifting of the Continuing Resolution, OIT now has approval to fill vacancies, but the federal IT team continues to be operating below its intended size while hiring actions are underway. Currently, the CISO position is vacant and a Privacy Lead position that had been gapped for 3 years onboarded in August 2022.

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

DFC | U.S. International Development Finance Corporation

- FY 22 was DFC's first year completely on its new domain, DFCNet - a domain migration from OPIC to DFC that was started in FY 21. This change in domain from OPICNet added strain to the agency's IT team as much of the required information security documentation needed to be updated and re-reviewed for the agency's FISMA reportable systems.

The FY 22 audit made six recommendations with which DFC immediately prioritized the strengthening of its information security program by implementing robust corrective actions to address the root causes of the findings. As of the date of this letter, DFC has fully completed its corrective actions over three of the six recommendations with partial corrective actions completed over another two recommendations. With swift action taken and close collaboration with our OIG, DFC was already able to obtain formal closure of recommendations #4 and #6 with the OIG and the agency's response to any remaining open recommendations provided below:

Universal response to all recommendations:

- DFC advertised and selected a new CISO to mature the information security program; planned start date in November 2022.
- DFC acquired contractor services to perform an independent FISMA readiness review and information security health assessment for FY 23; planned start date in October 2022.
- DFC reprioritized OIT hiring vacancies to increase federal staffing on the information security team.

OIG Recommendation No. 1: OIG recommends that the Chief Information Officer update its Authorization to Operate and system-level Security Assessment Reports annually.

Management Response: DFC concurs with the recommendation that we perform ongoing security control assessments and corrective actions have been partially completed. Specifically, DFC will adhere to an annual schedule to review and update its Authorization to Operate (ATOs) and system-level Security Assessment Reports (SARs) for our systems.

Responsible Party: Office of Information Technology

Target Resolution Date: The master schedule was completed in September 2022 and all outdated ATOs and SARs will be completed by FY 23 Q2

OIG Recommendation No. 2: OIG recommends that the Chief Information Officer implement a plan to replace or upgrade the unsupported software within DFC's network.

Management Response: DFC concurs with this recommendation to implement a plan to replace or upgrade unsupported software within the DFC's network. OIT will develop a methodology for assessing end of life software and to ensure end of life software is off our network and/or has a documented risk acceptance memo in place. A documented risk acceptance memo with mitigation steps has been in place on our

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

DFC | U.S. International Development Finance Corporation

Oracle EBS platform since October 2021. There is currently an active project to move this platform onto supported HW/SW targeting the end of December 2022 for completion.

Responsible Party: Office of Information Technology

Target Resolution Date: FY 23 Q2

OIG Recommendation No. 3: OIG recommends that the Chief Information Officer document and implement 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.

Management Response: DFC concurs with this recommendation and corrective actions have been fully completed.

Responsible Party: Office of Information Technology

Target Resolution Date: The recommendation will remain open until the next audit for final verification of the implementation of the lesson-learned requirements as defined in OIT's Continuous Monitoring Plan.

OIG Recommendation No. 4: OIG recommends that the Chief Information Officer perform data exfiltration/breach tabletop exercises annually.

Management Response: DFC concurred with this recommendation and corrective actions have been fully completed. OIT documented a process for annual data exfiltration/breach tabletop exercises and the first tests were performed in September 2022. Test results were submitted to the OIG for review and the recommendation was closed-out by the OIG in October 2022.

Responsible Party: Office of Information Technology

OIG Recommendation No. 5: OIG recommends that the Chief Information Officer develop a methodology and implement a tool to track the timely review of periodic updates for BIAs, and contingency tests.

Management Response: DFC concurs with this recommendation and corrective actions have been partially completed. A master schedule to perform updates and perform contingency tests is documented and the corrective action will be completed once contingency testing is performance in accordance with the schedule.

Responsible Party: Office of Information Technology

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

DFC | U.S. International Development Finance Corporation

Target Resolution Date: The master schedule was documented in October 2022. Contingency testing will be completed by FY 23 Q3.

OIG Recommendation No. 6: OIG recommends that the Chief Information Officer update DFC's Vulnerability and Risk Management Program to differentiate vulnerabilities remediation timeframe between internal and external facing systems and align with timeframes in the Department of Homeland Security's Fiscal Year 2022 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.

Management Response: DFC concurred with this recommendation and corrective actions have been fully completed. OIT updated its vulnerability mitigation policy to reflect DHS's metrics in September 2022 and the updated policy was approved by DFC management. The policy was submitted to the OIG for review and the recommendation was closed-out by the OIG in October 2022.

Responsible Party: Office of Information Technology

/s/

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 resolved to address two (2) out of the six (6) recommendations and outlined its plans to address the remaining four (4) recommendations. DFC's comments with redactions are included in Appendix II.

Based on our evaluation of management comments, we acknowledge DFC's management decisions on all six (6) recommendations and believe the actions taken and planned will resolve the issues identified in the report. Further, we determined that two (2)[16] out of the six (6) recommendations are closed with the issuance of this report. The remaining recommendations[17] are open pending the completion of planned activities.

[16] FY 2022-Recommendations 4 and 6
[17] FY 2022-Recommendations 1, 2, 3, and 5.