OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

DFC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA

Audit Report A-DFC-22-003-C
December 1, 2021

Information Technology Audit Division

MEMORANDUM

DATE: December 1, 2021

TO: DFC OIG, Inspector General, Anthony Zakel

FROM: Deputy Assistant Inspector General for Audit, Alvin A. Brown /s/

SUBJECT: DFC Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA (A-DFC-22-003-C)

Enclosed is the final audit report on the U. S. International Development Finance Corporation's (DFC's)[1] information security program for fiscal year (FY) 2021, in support of the Federal Information Security Modernization Act of 2014 (FISMA). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the audit. The contract required CLA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed CLA's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on DFC's compliance with FISMA. CLA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which CLA did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether DFC implemented an effective information security program.[2] To answer the audit objective, CLA evaluated the effectiveness of DFC's implementation of the FY 2021 IG FISMA reporting metrics[3] that fall into the nine domains in

[1] In October 2018, the passage of the Better Utilization of Investments Leading to Development Act (BUILD Act) established DFC, which combined the Overseas Private Investment Corporation's (OPIC) existing operations with USAID's Development Credit Authority. In accordance with the Act, the DFC Board of Directors appointed an Inspector General for DFC in late FY 2020, signifying the point for USAID OIG to begin transitioning out of its former oversight role for OPIC and current oversight role for DFC. USAID OIG completed selected mandated work for DFC oversight, concluding with this engagement, while DFC OIG built its capacity. DFC OIG began tracking and reporting open recommendations in its semi-annual report to Congress for the period ended September 30, 2021.

[2] For this audit, an effective information security program was defined as having an overall mature program based on the current year inspector general (IG) FISMA reporting metrics.

[3] Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," May 12, 2021.

the following table. Also, CLA assessed DFC's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." CLA reviewed three of the four internal and external systems in DFC's inventory dated February 12, 2021. Audit fieldwork covered DFC's headquarters located in Washington, DC, from April 13, 2021, to August 11, 2021, for the period from October 1, 2020, through August 11, 2021.

The audit firm concluded that DFC implemented an effective information security program. For example, DFC:

- Established an effective security training program.
- Maintained an effective information system continuous monitoring program.
- Implemented an effective incident handling and response program

However, as summarized in the table below, CLA noted weaknesses in four of the nine FY 2021 IG FISMA metric domains.

Fiscal Year 2021 IG FISMA Metric Domains	**Weaknesses Identified**
Risk Management	
Supply Chain Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	X
Security Training	
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	

To address the weaknesses identified in CLA's report, we recommend that DFC's Chief Information Officer take the following actions:

Recommendation 1. Develop and implement a process to include compensating controls to mitigate risk when accepting the risk of known vulnerabilities.

Recommendation 2. Document and implement a process to verify that laptops are encrypted and remediate instances of nonencrypted laptops.

Recommendation 3. Document and implement a strategy, policy, and procedures to manage supply chain risks with suppliers, contractors, and systems.

In addition, DFC took corrective action and closed 9 of 13 open recommendations from the FY 2017[4], 2018[5], 2019[6] and FY 2020[7] FISMA audit reports. Refer to Appendix III on page 15 of CLA's report for the full text and status of prior year recommendations.

In finalizing the report, the audit firm evaluated DFC's responses to the recommendations. After reviewing that evaluation, we consider all three recommendations resolved but open pending DFC OIG's verification of the agency's final actions. Please provide evidence of final action to DFC OIG.

We appreciate the assistance provided to our staff and the audit firm's employees during the engagement.

[4] Recommendation 1 in USAID OIG, "OPIC Implemented Controls in Support of FISMA for Fiscal Year 2017 But Improvements Are Needed" (A-OPC-17-007-C), September 28, 2017.
[5] Recommendations 1, 2, 3, 4 and 7 in USAID OIG, "OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018" (A-OPC-19-006-C), January 30, 2019.
[6] Recommendations 2, 3 and 4 in USAID OIG, "OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019" (A-OPC-20-003-C), January 16, 2020.
[7] Recommendations 1, 2, 3 and 4 in USAID OIG, "DFC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA" (A-DFC-21-005-C), January 28, 2021.

United States International Development Finance Corporation's Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2021

Final Report

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

phone 571-227-9500 **fax** 571-227-9552
CLAconnect.com

November 30, 2021

Ms. Lisa Banks
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20005-2221

Dear Ms. Banks:

CliftonLarsonAllen LLP (CLA) is pleased to present our final report on the results of our audit of the United States International Development Finance Corporation's (DFC) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2021.

We appreciate the assistance we received from DFC. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
United States Agency for International Development

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the United States International Development Finance Corporation's (DFC) information security program and practices for fiscal year 2021 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an Agency-wide information security program and practices. The Act also requires Inspectors General (IG) to conduct an annual review of their agencies' information security program and report the results to the Office of Management and Budget (OMB).

The objective of this performance audit was to determine whether DFC implemented an effective information security program. For this audit, an effective information security program was defined as having an overall mature program based on the current year IG FISMA reporting metrics.

For this year's review, OMB required IGs to assess 66 metrics in the following five security function areas to determine the effectiveness of their agencies' information security program and the maturity level of each function area: Identify, Protect, Detect, Respond, and Recover. The maturity levels, ranging from lowest to highest are 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. The scope also included assessing selected security controls outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of 3 of 4 internal and external systems in DFC's FISMA inventory of information systems.

Audit fieldwork covered DFC's headquarters located in Washington, DC, from April 13, 2021, to August 11, 2021. It covered the period from October 1, 2020, through August 11, 2021.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We concluded that DFC implemented an effective information security program by achieving an overall *Managed and Measurable* maturity level based on the FY 2021 IG FISMA reporting metrics. Although we concluded that DFC implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted four weaknesses that fell in the supply chain risk management, configuration management, identity and access management, and data protection and privacy domains of

the FY 2021 IG FISMA reporting metrics and have made three recommendations to assist DFC in strengthening its information security program. In addition, we noted four 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. CLA 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 November 30, 2021. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to November 30, 2021.

The purpose of this audit report is to report on our assessment of DFC's compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations are included in the accompanying report. We are submitting this report to the USAID Office of Inspector General.

CliftonLarsonAllen LLP

Arlington, Virginia
November 30, 2021

TABLE OF CONTENTS

SUMMARY OF RESULTS

Background

The United States Agency for International Development (USAID) Office of Inspector General engaged us to conduct an audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an annual evaluation of the U.S. International Development Finance Corporation's (DFC or Corporation) information security program and practices. The objective of this performance audit was to determine whether DFC implemented an effective information security program.[2]

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires federal agencies to develop, document, and implement an Agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget (OMB) and to congressional committees on the effectiveness of their information security program.

FISMA also requires agency Inspectors General (IGs) to assess the effectiveness of agency information security programs and practices. OMB and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

OMB and the Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On November 9, 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete IG FISMA reporting metrics[3] to independently assess their agencies' information security program.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of OMB with respect to Agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] For this audit, an effective information security program is defined as having an overall mature program based on the current year Inspector General (IG) FISMA reporting metrics.

[3] We will submit the responses to the FY 2021 IG FISMA reporting metrics to USAID Office of Inspector General as a separate deliverable under the contract for this performance audit.

As highlighted in Table 1, the fiscal year (FY) 2021 IG FISMA reporting metrics are designed to assess the maturity of the information security program and align with the five function areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover. The FY 2021 IG FISMA reporting metrics include Supply Chain Risk Management (SCRM), a new domain within the Identify function area; however, the SCRM domain was not considered in the Identify framework function rating.

For FY 2021, OMB required IGs to assess 66 metrics in the five security function areas to determine the effectiveness of their information security program and the maturity level of each function area.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2021 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metric Domains
Identify	Risk Management, Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

For this audit, we reviewed selected controls[4] mapped to the FY 2021 IG FISMA reporting metrics for a sample of 3 of 4 internal and external information systems[5] in DFC's FISMA inventory as of February 12, 2021.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[4] The controls were tested to the extent necessary to determine whether DFC implemented the processes specifically addressed in the IG FISMA reporting metrics. In addition, not all controls were tested for all three sampled information systems since several controls were inherited from the DFC general support system and certain controls were not applicable for external systems.

[5] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Audit Results

We concluded that DFC implemented an effective information security program by achieving an overall *Managed and Measurable* maturity level based on the FY 2021 IG FISMA reporting metrics.[6] For example, DFC:

- Established an effective security training program.
- Maintained an effective information system continuous monitoring program.
- Implemented an effective incident handling and response program.

Table 2 below shows a summary of the overall maturity levels for each domain and function area in the FY 2021 IG FISMA reporting metrics.

Table 2: Maturity Levels for the FY 2021 IG FISMA Reporting Metrics

Security Function	FY 2021 Maturity Level by Function	Metric Domains	Maturity Level by Domain
Identify	Consistently Implemented	**Risk Management**	Consistently Implemented
		Supply Chain Risk Management	Ad Hoc[7]
Protect	Managed and Measurable	**Configuration Management**	Managed and Measurable
		Identity and Access Management	Optimized
		Data Protection and Privacy	Defined
		Security Training	Managed and Measurable
Detect	Managed and Measurable	**Information Security Continuous Monitoring**	Managed and Measurable
Respond	Managed and Measurable	**Incident Response**	Managed and Measurable
Recover	Consistently Implemented	**Contingency Planning**	Consistently Implemented
Overall	**Level 4: Managed and Measurable - Effective**		

Although we concluded that DFC implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted four weaknesses in the SCRM, configuration management, identity and access management, and data protection and privacy domains of the FY 2021 IG FISMA reporting metrics (see Table 3) and are making three new recommendations to assist DFC in strengthening its information security program. In addition, we noted four recommendations in prior FISMA audits remain open.

[6] In accordance with the FY 2021 FISMA reporting metrics, ratings throughout the nine domains were determined by a simple majority, where the most frequent level across the questions served as the domain rating. Agencies were rated at the higher level in instances when two or more levels were the most frequently rated. The domain ratings inform the overall function ratings, and the five function ratings inform the overall agency rating.

[7] The FY 2021 IG FISMA reporting metrics indicated that, to provide agencies with sufficient time to fully implement NIST Special Publication 800-53, Revision 5, in accordance with OMB A-130, these new metrics should not be considered for the purposes of the Identify framework function rating, and therefore would not be considered for the overall rating.

Table 3: Weaknesses Noted in the FY 2021 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	None
	Supply Chain Risk Management	DFC Needs to Implement a Supply Chain Risk Management Strategy (**See Finding # 4**)
Protect	**Configuration Management**	DFC Needs to Strengthen Vulnerability and Patch Management Controls **(See Finding # 1)**
	Identity and Access Management	DFC Needs to Fully Implement Multifactor Authentication for Privileged Users **(See Finding # 2)**
	Data Protection and Privacy	DFC Needs to Fully Implement Encryption on Laptops **(See Finding # 3)**
	Security Training	None
Detect	**Information Security Continuous Monitoring**	None
Respond	**Incident Response**	None
Recover	**Contingency Planning**	None

In addition, DFC[8] took corrective action to address and close 9 recommendations from the FY 2018,[9] FY 2019,[10] and FY 2020[11] FISMA audits. Refer to Appendix III for the status of prior year recommendations.

In response to the draft report, DFC outlined and described its plans to address all three recommendations. Based on our evaluation of management comments, we acknowledge DFC's management decisions on all three recommendations. Further, we consider these recommendations resolved, but open pending completion of planned activities. DFC's comments are included in their entirety in Appendix II. The following section provides a detailed discussion of the audit findings. Appendix I describes the audit scope and methodology.

[8] In 2019, DFC was established by combining Overseas Private Investment Corporation (OPIC) and the Development Credit Authority. Therefore, DFC inherited responsibility for implementing prior audit recommendations that were addressed to OPIC.
[9] *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019).
[10] *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-OPC-20-003-C, January 16, 2020).
[11] *DFC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-DFC-21-005-C, January 28, 2021).

AUDIT FINDINGS

1. DFC Needs to Strengthen Vulnerability and Patch Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Metric Domain: *Configuration Management*

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* security control System and Information Integrity SI-2, states the following regarding flaw remediation:

> The organization:
> * * *
> c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
> d. Incorporates flaw remediation into the organizational configuration management process.

Also, OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix I, states:

> i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems.
>
> Agencies shall:
> * * *
> 8. Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement; and
> 9. Implement and maintain current updates and patches for all software and firmware components of information systems.

In addition, NIST SP 800-53, Revision 4, states the following regarding the compensating controls:

> *Selecting Compensating Security Controls:*
>
> Organizations may find it necessary on occasion to employ compensating security controls. Compensating controls are alternative security controls employed by organizations. Compensating controls may be employed by organizations under the following conditions:
>
> - Select compensating controls…if appropriate compensating controls are not available, organizations adopt suitable compensating controls from other sources;
> - Provide supporting rationale for how compensating controls provide equivalent security capabilities for organizational information systems and why the baseline security controls could not be employed; and

- Assess and accept the risk associated with implementing compensating controls in organizational information systems.

We performed independent scans using the software tool Nessus[12] and noted critical and high vulnerabilities on one of DFC's systems in scope. Those vulnerabilities were from 2020 and earlier and related to missing patches, configuration weaknesses, and unsupported software.

DFC documented a risk acceptance for unsupported operating systems and software, which included plans to replace known vulnerable and unsupported software as replacement software is procured and implemented. However, the risk acceptance does not document mitigating controls such as isolation or access restriction to the vulnerable devices. Further, DFC did not include all critical and high vulnerabilities in the risk acceptance decisions, including missing patches and configuration weaknesses. This occurred because DFC did not implement a process to include mitigating controls for risk acceptance.

Unmitigated vulnerabilities on DFC's network can compromise the confidentiality, integrity, and availability of information on the network. For example:

- An attacker may leverage known vulnerabilities to execute arbitrary code.
- Authorized DFC employees may be unable to access systems.
- DFC data may be lost, stolen, or compromised.

Furthermore, unsupported systems may be susceptible to older vulnerabilities and exploits that vendors have addressed with current supported versions.

Recommendations addressing the vulnerabilities were issued in the FY 2017[13] and FY 2018[14] FISMA audits and have not been fully remediated. However, to address the weakness that the risk acceptances for unsupported software did not include compensating controls to mitigate the risks, we are making the following recommendation:

> ***Recommendation 1:*** *We recommend that DFC's Chief Information Officer develop and implement a process to include compensating controls to mitigate risk when accepting the risk of known vulnerabilities.*

[12] Nessus is a vulnerability scanner developed by Tenable, Inc.
[13] Recommendation 1, *OPIC Implemented Controls in Support of FISMA for Fiscal Year 2017 but Improvements Are Needed* (Audit Report No. A-OPC-17-007-C, September 28, 2017).
[14] Recommendation 2 and 3, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019).

2. DFC Needs to Fully Implement Multifactor Authentication for Privileged Users

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Metric Domain: *Identity and Access Management*

NIST SP 800-53, Revision 4, security control Identification and Authentication IA-2, states the following regarding multifactor authentication:

> * * *
>
> Control Enhancement:
>
> * * *
>
> 2. The information system implements multifactor authentication for network access to privileged accounts.

Multifactor authentication was not enforced for network access for privileged accounts. The enforcement of multifactor authentication for server administrator network access was pending the completion of the transfer from the OPIC domain to the DFC domain.

By not fully implementing multifactor authentication on servers for privileged users, there is an increased risk that unauthorized individuals may compromise passwords and gain access to the information system or the information system data.

A recommendation addressing this finding was issued in the FY 2020 FISMA audit[15] and has not been fully remediated. Therefore, we are not making a new recommendation.

3. DFC Needs to Fully Implement Encryption on Laptops

Cybersecurity Framework Security Function: *Protect*
FY 2021 FISMA IG Metric Domain: *Data Protection and Privacy*

NIST SP 800-53, Revision 4, security control Access Control AC-19, states the following regarding encryption for mobile devices:

> * * *
>
> Control Enhancement:
>
> * * *
>
> 5. The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

DFC's *NIST 800-53 Security Controls OPIC*[16] *Organizational Parameters*, AC-19, states:

> The organization employs Full Device Encryption or Container Encryption to protect the confidentiality and integrity of information on all mobile devices approved to access OPIC networks and systems.

[15] Recommendation 3, *DFC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-DFC-21-005-C, January 28, 2021).
[16] The Better Utilization of Investments Leading to Development (BUILD) Act, signed on October 5, 2018, resulted in the combination of the Overseas Private Investment Corporation (OPIC) and USAID's Development Credit Authority into DFC at the beginning of Fiscal Year 2020.

We performed independent scans using the software tool Nessus and noted that 6 of the 20 windows workstations identified by the scans were not encrypted. Further, 5 of the 6 devices were identified as laptops. After identification, DFC management indicated that there was a visibility issue with their recently implemented monitoring tool where unencrypted laptops were presented as encrypted in its dashboard. DFC indicated they were working with the vendor to address the inconsistent reporting. This occurred because DFC did not implement a process to verify that laptops are encrypted.

Without encrypting mobile devices such as laptops, DFC may lose the confidentiality of sensitive data if a laptop is lost or stolen. Therefore, we are making the following recommendation:

> ***Recommendation 2:*** *We recommend that DFC's Chief Information Officer document and implement a process to verify that laptops are encrypted and remediate instances of nonencrypted laptops.*

4. DFC Needs to Implement a Supply Chain Risk Management Strategy

Cybersecurity Framework Security Function: *Identify*
FY 2021 FISMA IG Metric Domain: *Supply Chain Risk Management*

Public Law 115-390 – 115th Congress, Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the ''SECURE Technology Act" (12/31/18) states:

> *§1326 (a). Requirements for executive agencies*
>
> (a) In General. —The head of each executive agency shall be responsible for—
> (1) assessing the supply chain risk posed by the acquisition and use of covered articles and avoiding, mitigating, accepting, or transferring that risk, as appropriate and consistent with the standards, guidelines, and practices identified by the Council under section 1323(a)(1); and (2) prioritizing supply chain risk assessments conducted under paragraph (1) based on the criticality of the mission, system, component, service, or asset.
>
> (b) Inclusions. —The responsibility for assessing supply chain risk described in subsection (a) includes—(1) developing an overall supply chain risk management strategy and implementation plan and policies and processes to guide and govern supply chain risk management activities.

In addition, NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Chapter 2, section 2.2.1 FRAME, states:

> An organization Information and Communication Technology (ICT) SCRM policy is a critical vehicle for guiding ICT SCRM activities. Driven by applicable laws and regulations, this policy should support applicable organization policies including acquisition and procurement, information security, quality, and supply chain and logistics. It should address goals and objectives articulated in the overall agency strategic plan, as well as specific mission functions and business goals, along with

the internal and external customer requirements. It should also define the integration points for ICT SCRM with the agency's Risk Management Process and System Development Life Cycle (SDLC).

DFC has not documented a SCRM strategy, policies, or procedures. DFC relies on procuring supplies and contractors through National Aeronautics and Space Administration's Solution for Enterprise-Wide Procurement (SEWP) and General Services Administration to reduce associated SCRM risks. However, this strategy and the associated policies and procedures have not been documented.

As a result, DFC is at risk of implementing SCRM related policies and procedures which are not effectively integrated into DFC's risk management processes or appropriately tailored to DFC's specific mission/business needs. Therefore, we are making the following recommendation:

Recommendation 3: *We recommend that DFC's Chief Information Officer document and implement a strategy, policy and procedures to manage supply chain risks with suppliers, contractors and systems.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, DFC outlined its plans to address all three recommendations. DFC's comments are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge DFC's management decisions on all three recommendations. Further, we consider these recommendations resolved, but open pending completion of planned activities.

SCOPE AND METHODOLOGY

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

The audit was designed to determine whether DFC implemented an effective information security program. For this audit, an effective information security program was defined as having an overall mature program based on the current IG FISMA reporting metrics.

For this year's review, Inspectors General were to assess 66 metrics in five security function areas to determine the effectiveness of their agencies' information security program and the maturity level of each function area: Identify, Protect, Detect, Respond, and Recover. The maturity levels ranging from lowest to highest are Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

The scope of this performance audit was to assess DFC's information security program consistent with FISMA, and reporting instructions issued by OMB and DHS. The scope also included assessing selected security controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of 3 of 4 internal and external information systems[17] in DFC's FISMA inventory as of February 12, 2021.

In addition, we performed an internal vulnerability assessment of DFC's network.

The audit also included a follow up on prior audit recommendations (2017,[18] 2018,[19] 2019,[20] and 2020[21]) to determine whether DFC made progress in implementing them. See Appendix III for the status of prior year recommendations.

Audit fieldwork covered DFC's headquarters located in Washington, DC, from March 31, 2021, to August 11, 2021. It covered the period from October 1, 2020, through August 11, 2021.

[17] Ibid 5.
[18] *OPIC Implemented Controls in Support of FISMA for Fiscal Year 2017 but Improvements Are Needed* (Audit Report No. A-OPC-17-007-C, September 28, 2017).
[19] Ibid 9.
[20] Ibid 10.
[21] Ibid 11.

Methodology

To determine if DFC implemented an effective information security program, we conducted interviews with DFC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, we reviewed documents supporting the information security program. These documents included, but were not limited to, DFC's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, we compared documents, such as DFC's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls. We also reviewed the status of FISMA audit recommendations from fiscal year 2017, 2018, 2019, and 2020.[22]

In testing the effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity (not the percentage of deficient items found compared to the total population available for review). In some cases, this resulted in selecting the entire population. However, in cases where the entire audit population was not selected, the results cannot be projected and if projected may be misleading.

To perform our audit of DFC's information security program and practices, we followed a work plan based on, but not limited to, the following guidance:

- OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB and DHS, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource.*
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- 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 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*

[22] Ibid 18, 9, 10, and 11.

MANAGEMENT COMMENTS

MEMORANDUM October 29, 2021

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

FROM: Tina Donbeck
Chief Information Officer (CIO)
DFC – Office of Information Technology

SUBJECT: DFC Comments on the Audit of the US International Development Finance Corporation's Fiscal Year 2021 Compliance with Provisions of the Federal Information Security Modernization Act of 2014

Below is the DFC's response to the Office of Inspector General's (OIG) DRAFT report DFC Generally Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA

The Inspector General report contains three (3) new recommendations for corrective action. This memorandum provides DFC's management responses to these recommendations.

Recommendation No. 1: We recommend that DFC's Chief Information Officer develop and implement a process to include compensating controls to mitigate risk when accepting the risk of known vulnerabilities.

Management Response: The OIT agrees with this recommendation and has updated the DFC Risk and Vulnerability Management procedure to identify critical and high vulnerabilities and list the associated compensating controls in risk acceptance memos. This will ensure that the relevant information is reviewed during the risk acceptance process. **Completion Date: 10/15/21.** The CISO team will submit the closure memo with the appropriate evidence showing the process is in place.

Recommendation No. 2: We recommend that DFC's Chief Information Officer document and implement a process to verify that laptops are encrypted and remediate instances of nonencrypted laptops.

Management Response: The OIT agrees with this finding. The six devices listed from the sample have now been encrypted. OIT has reviewed and updated the DFC Imaging Process document used to verify that laptops are encrypted as part of the imaging and deployment process. OIT has a process using BigFix to report on current encryption state of all in production laptops. Any laptops that are out of compliance are reported to the DFC service desk for remediation. **Completion Date: 10/19/21.** The CISO team will submit the closure memo with the appropriate evidence showing the process is in place.

Recommendation No. 3: We recommend that DFC's Chief Information Officer document and implement a strategy, policy and procedures to manage supply chain risks with suppliers, contractors and systems.

Management Response: The OIT agrees with this recommendation and has developed a DFC Supply Chain Risk Management Strategy Policy and accompanying procedures. **Completion Date 10/14/21.** The CISO team will submit the closure memo with the appropriate evidence showing the process is in place.

/s/

STATUS OF PRIOR YEAR RECOMMENDATIONS

The following tables provide the status of the FY 2017, FY 2018, FY 2019, and FY 2020[23] FISMA audit recommendations.

No.	FY 2017 Audit Recommendation	DFC Position on Status	Auditor's Position on Status
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 – See finding 1

No.	FY 2018 Audit Recommendation	DFC Position on Status	Auditor's Position on Status
1	Document and implement a process to update its privacy impact assessments for the Corporation's information systems.	Closed	Agree
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 - See finding 1
3	Document and implement a process to verify that patches are applied in a timely manner.	Open	Agree – See finding 1
4	Document and implement a process to verify that (1) the account management system is updated promptly to support the management of information system accounts and (2) inactive accounts are promptly disabled after 30 days in accordance with the Corporation's access control procedures.	Closed	Agree
7	Conduct (1) contingency training and (2) a test of the information system contingency plan in accordance with OPIC's policy.	Closed	Agree

No.	FY 2019 Audit Recommendation	DFC Position on Status	Auditor's Position on Status
2	Implement asset management procedures to include processes for ensuring information system assets are inventoried on an organization-defined frequency.	Closed	Agree
3	Complete the enterprise architecture strategy to be in line with the Federal enterprise architecture and risk management framework.	Closed	Agree
4	Document and implement a process to verify oversight of information technology-related contractor roles and responsibilities.	Closed	Agree

[23] Ibid 18, 9, 10, and 11.

No.	FY 2020 Audit Recommendation	DFC Position on Status	Auditor's Position on Status
1	Review and update privacy policies and breach response procedures to accurately reflect the Corporation's operating environment.	Closed	Agree
2	Implement a process to validate completion of rules of behavior and security and privacy awareness training prior to providing system access.	Closed	Agree
3	Implement multifactor authentication for network access for privileged accounts.	Open	Agree – See finding 2
4	Implement session disconnect for virtual private network connections to be compliance with DFC requirements.	Closed	Agree