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

DFC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA

AUDIT REPORT A-DFC-21-005-C
JANUARY 28, 2021

1300 Pennsylvania Avenue NW • Washington, DC 20523
https://oig.usaid.gov • 202-712-1150

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, Millennium Challenge Corporation, U.S. African Development Foundation, U.S. International Development Finance Corporation, and Inter-American Foundation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: ig.hotline@usaid.gov
Complaint form: https://oig.usaid.gov/complainant-select
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: January 28, 2021

TO: DFC OIG, Inspector General, Anthony Zakel

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

SUBJECT: DFC Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA (A-DFC-21-005-C)

Enclosed is the final audit report on the U.S. International Development Finance Corporation's (DFC)[1] information security program for fiscal year 2020, 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 tested DFC's implementation of

[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 will continue to complete selected mandated work for DFC oversight while DFC's Office of the Inspector General builds its capacity.

[2] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

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 auditors reviewed all three information systems in DFC's inventory dated May 2020. Fieldwork covered DFC's headquarters in Washington, DC, from May 7 to September 1, 2020. It covered the period from October 1, 2019, through September 1, 2020.

The audit firm concluded that DFC generally implemented an effective information security program by implementing 66 of 75[3] instances of selected security controls for selected information systems. Among those controls, DFC maintained an effective:

- Information system continuous monitoring program.
- Incident handling and response program.
- Contingency planning program.

However, as summarized in the table below, CLA noted weaknesses in five of the eight FISMA metric domains.

Fiscal Year 2020 IG FISMA Metric Domains[4]	**Weaknesses Identified**
Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	X
Security Training	X
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: Review and update privacy policies and breach response procedures to accurately reflect the Corporation's operating environment.

Recommendation 2: Implement a process to validate completion of rules of behavior and security and privacy awareness training prior to providing system access.

[3] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the fiscal year 2020 IG metrics. CLA tested 66 controls. A control was counted for each system it was tested against. Thus, there were 75 instances of testing a control.

[4] The Office of Management and Budget, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency's "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," (April 17, 2020).

Recommendation 3: Implement multifactor authentication for network access for privileged accounts.

Recommendation 4: Implement session disconnect for virtual private network connections to comply with DFC requirements.

In addition, DFC had not taken final corrective action on nine recommendations made in our 2017[5], 2018[6] and 2019[7] FISMA audit reports. Since the recommendations had not been closed, we are not repeating them for any current weaknesses in this report. See Appendix IV on page 20 of CLA's report for the full text of the recommendations.

In finalizing the report, the audit firm evaluated DFC's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1 and 3 resolved but open pending completion of planned activities, and recommendations 2 and 4 resolved but open pending OIG's verification of the agency's final actions. Please provide evidence of final action to OIGAuditTracking@usaid.gov.

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

[5] 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.

[6] 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.

[7] 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.

United States International Development Finance Corporation's

Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2020

Final Report

A member of Nexia International

CliftonLarsonAllen LLP
CLAconnect.com

January 19, 2021

Mr. Mark Norman
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, D.C. 20005-2221

Dear Mr. Norman:

CliftonLarsonAllen LLP (CLA) is pleased to present our 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 2020.

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

Very truly yours,

S. M Mirzakhani

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 2020 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether DFC implemented an effective information security program. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls for all three of DFC's internal and external information systems. For this year's review, Inspectors General (IGs) were also required to assess information security programs on a maturity scale from Level 1 (Ad Hoc) to Level 5 (Optimized) in eight IG FISMA Metric Domains and five Function areas – Identify, Protect, Detect, Respond, and Recover – to determine the effectiveness of their agencies' information security programs and the maturity level of each function area.

Audit fieldwork covered DFC's headquarters located in Washington, DC, from May 7, 2020 to September 1, 2020. It covered the period from October 1, 2019, through September 1, 2020.

We conducted our 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 generally implemented an effective information security program by implementing many of the selected security controls for selected information systems. Although DFC generally implemented an effective information security program, its implementation of a subset of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in five of the eight Inspector General FISMA Metric Domains and have made four new recommendations to assist DFC in strengthening its information security program. In addition, we noted that nine recommendations related to prior year FISMA audits were still 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 January 19, 2021. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to January 19, 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

CliftonLarsonAllen LLP

Arlington, Virginia
January 19, 2021

TABLE OF CONTENTS

SUMMARY OF RESULTS

Background

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) 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)[2] information security program and practices. The objective of this performance audit was to determine whether DFC implemented an effective[3] information security program.

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 19, 2019, OMB issued Memorandum M-20-04, *Fiscal Year 2019-2020 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[4] to independently assess their agencies' information security programs.

---

[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] 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.

[3] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

[4] CLA submitted its responses to the FY 2020 IG FISMA Reporting Metrics to USAID OIG as a separate deliverable under the contract for this performance audit.

The fiscal year (FY) 2020 IG FISMA Reporting Metrics are designed to assess the maturity[5] of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover, as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2020 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2020 IG FISMA Reporting Metric Domains
Identify	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, CLA reviewed selected[6] controls related to the IG FISMA Reporting Metrics from all three information systems[7] in DFC's FISMA inventory as of May 2020.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. CLA believes that the evidence obtained provides a reasonable basis for CLA's findings and conclusions based on the audit objective.

Audit Results

We concluded that DFC generally implemented an effective information security program by implementing 66 of 75[8] selected security and privacy control instances for selected information systems. For example, DFC:

- Maintained an effective information system continuous monitoring program.
- Maintained an effective incident handling and response program.
- Maintained an effective contingency planning program.

Although DFC generally implemented an effective information security program, its implementation of 9 of the 75 control instances was not fully effective to preserve the

[5] The five levels in the maturity model are: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized.
[6] See Appendix III for a list of controls selected.
[7] 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.
[8] There were 86 NIST SP 800-53, Revision 4, controls, including enhancements, specifically identified in the FY 2020 IG metrics. We tested 66 controls. A control was counted for each system it was tested against. Thus, there were 75 instances of testing a control. See Appendix III for a list of the controls.

confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. As a result, CLA noted weaknesses in the following FISMA Metric Domains (Table 2) and made four recommendations to assist DFC in strengthening its information security program.

Table 2: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2020 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2020 IG FISMA Metric Domains	Weaknesses Noted in FY 2020
Identify	**Risk Management**	DFC Needs to Strengthen its Enterprise Architecture Strategy (**Finding 8**)
Protect	**Configuration Management**	DFC Needs to Strengthen Vulnerability and Patch Management Controls **(Finding 1)** DFC Needs to Strengthen Asset Management Controls (**Finding 3**)
	Identity and Access Management	DFC Needs to Strengthen Account Management Controls (**Finding 2**) DFC Needs to Fully Implement Multifactor Authentication for Privileged Users (**Finding 6**) DFC Needs to Strengthen Remote Access Controls (**Finding 7**)
	Data Protection and Privacy	DFC Needs to Ensure Privacy Program Documentation is Up-to-Date (**Finding 4**)
	Security Training	DFC Needs to Strengthen Personnel Onboarding Training Requirements (**Finding 5**)
Detect	**Information Security Continuous Monitoring**	None
Respond	**Incident Response**	None
Recover	**Contingency Planning**	None

In response to the draft audit report, DFC provided plans to implement each of the recommendations 1, 2, 3, and 4, but did disagree with part of recommendation 2. Based on our evaluation of management's comments, we acknowledge DFC's management decisions on recommendations 1, 2, 3 and 4. Further, we consider recommendations 1 and 3 resolved, but open pending completion of planned activities. In addition, we consider recommendations 2 and 4 open-resolved pending OIG's verification of the Agency's final actions. 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, Appendix II includes DFC management comments, Appendix III identifies the controls selected for testing, and Appendix IV provides the status of prior year recommendations.

AUDIT FINDINGS

1. DFC Needs to Strengthen Vulnerability and Patch Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 2020 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 patch management:

> The organization:
> * * *
> c. Installs security-relevant software and firmware updates within [*Assignment: organization defined time-period*] of the release of the updates.

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, 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.

CLA performed independent scans using the software tool Nessus[9] and noted vulnerabilities on one of DFC's systems in scope. CLA noted critical and high vulnerabilities from 2019 and earlier that related to missing patches, configuration weaknesses, and unsupported software.

Early in FY 2019, DFC began a process to identify vulnerabilities that were outside of specified remediation timeframes; however, we noted that the timely remediation of vulnerabilities remains delayed. DFC was aware of the identified vulnerabilities and has documented a plan to remediate vulnerabilities in a defined timeframe; however, older vulnerabilities and configuration weaknesses remain.

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.

[9] Nessus is a vulnerability scanner developed by Tenable, Inc.

- 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 this finding were issued in the FY 2018 FISMA audit[10] and have not been fully remediated. Therefore, we are not making a new recommendation.

2. DFC Needs to Strengthen Account Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 2020 FISMA IG Metric Domain: *Identity and Access Management*

NIST SP 800-53, Revision 4, Access Control (AC)-2, states the following regarding account management:

> The organization:
>
> * * *
>
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].
>
> h. Notifies account managers:
> 1. When accounts are no longer required;
> 2. When users are terminated or transferred; and
> 3. When individual information system usage or need-to-know changes.

Controls were not adequate to ensure DFC performed effective account management controls. Specifically, we noted the following account management weaknesses for inactive and terminated users for one sampled system:

- From a population of 465 Non-Privileged user accounts, 3 test accounts were not disabled after 30 days of inactivity in accordance with DFC's policy for the system.
- From a population of 41 Privileged user accounts, 1 account was not disabled after 30 days of inactivity in accordance with DFC's policy for the system.

The accounts identified were moved to a Deleted Organizational Unit[11] without being disabled or deleted. These accounts appear as active accounts in Active Directory.

In addition, from a population of 105 separated users, 9 out of 11 sampled terminated user accounts did not have evidence of accounts disabled in a timely manner. Specifically, DFC tracks employee separations through its human resources tool; however, these accounts were not consistently disabled timely or recorded in the system as having cleared the Helpdesk for account disabling. Further, DFC did not have an alternative method of showing that accounts were disabled timely for separated personnel.

[10] 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).

[11] In Microsoft's Active Directory, Organizational Units contain different objects from a domain allowing provisioning of configurations and permission by unit.

Without effective access controls, DFC information is at risk of unauthorized access, increasing the likelihood of unauthorized modification, loss, and disclosure. Inactive accounts that are not disabled in accordance with Agency policy and user accounts that are not disabled when employees separate may be used to gain access to the Agency's data and sensitive information.

A recommendation addressing this finding was issued in the fiscal year 2018 FISMA audit.[12] Since the recommendation remains open, we are not making a new recommendation.

3. DFC Needs to Strengthen Asset Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 2020 FISMA IG Metric Domain: *Configuration Management*

NIST SP 800-53, Revision 4, security control Configuration Management (CM)-8, states the following regarding information system component inventory:

> The organization:
> * * *
> b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].
>
> Control Enhancements:
> 1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates changes.

DFC's *NIST 800-53 Security Controls OPIC[13] Organizational Parameters*, CM-8, states, "Reviews and updates the information system component inventory quarterly."

DFC had not completed wall-to-wall hardware inventories on a quarterly basis as defined in its *Information System Security Policy* and *NIST 800-53 Security Controls OPIC Organizational Parameters*. DFC drafted a revised asset management policy to implement incremental inventories quarterly and a full inventory annually; however, the policy had not been fully implemented and the parameters were not updated to match the policy.

Without maintaining an updated component inventory, DFC is more susceptible to lost or misplaced assets that may result in unauthorized access to DFC data.

A recommendation addressing this finding was issued in the fiscal year 2019 FISMA audit.[14] Since that recommendation remains open, we are not making a new recommendation.

---

[12] Recommendation 4, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019).
[13] OPIC was the Overseas Private Investment Corporation which was one of the preceding government organizations that became DFC.
[14] Recommendation 2, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-OPC-20-003-C, January 16, 2020).

4. DFC Needs to Ensure Privacy Program Documentation is Up-to-Date

Cybersecurity Framework Security Function: *Protect*
FY 2020 FISMA IG Metric Domain: *Data Protection and Privacy*

NIST SP 800-53, Revision 4, privacy control Accountability, Audit, and Risk Management (AR)-2, states the following regarding privacy impact and risk assessment:

> The organization:
> * * *
> b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

In addition, privacy control Security (SE)-2, states the following regarding privacy incident response:

> The organization:
>
> a. Develops and implements a Privacy Incident Response Plan; and
> b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, dated January 3, 2017, states, "At the end of each fiscal year, the [Senior Agency Official for Privacy] shall review the reports from the principal SOC, described in Section VIII of this Memorandum, detailing the status of each breach reported during the fiscal year and consider whether the agency should undertake any of the following actions:

- Update its breach response plan;
- Develop and implement new policies to protect the agency's Personally Identifiable Information (PII) holdings;
- Revise existing policies to protect the agency's PII holdings;
- Reinforce or improve training and awareness;
- Modify information sharing arrangements; and
- Develop or revise documentation such as System of Records Notices (SORNs), PIAs, or privacy policies."

DFC's *Privacy Policy*, Section 7.2 Privacy Impact Assessments, states "(2) As determined by the PTA,[15] conduct PIAs of the systems every three years or when a change occurs as defined by NIST SP 800-53a, Guide for Assessing the Security Controls in Federal Information System, that creates a new privacy risk." In addition, System Owners must, "(4) review and revalidate the contents of their systems' PIA(s) biennially, or upon significant changes as needed, and document the results of each PIA review."

[15] A PTA is completed to determine what Personally Identifiable Information is contained in the system.

DFC's *Privacy Breach Notification Procedures*, Section 7: Effective Date, states, "The effective date is the date of issuance. This policy will be reviewed every two years to determine whether changes are necessary."

DFC has not conducted PIAs for two systems in over three years as required by its *Privacy Policy*. The two PIAs were last reviewed in FY 2012. DFC had implemented a notification process for PIAs that were out of date and had updated the PIA for one system; however, two outdated PIAs remained.

Due to an oversight as the agency transitioned from OPIC to DFC, the *Privacy Policy* and *Privacy Breach Notification Procedures* were carried over from the prior agency without review or update as required. In addition, DFC's *Privacy Policy* had not been reviewed or updated since the policy's creation or the DFC's *Privacy Breach Notification Procedures* since October 2010 in accordance with DFC policy. Furthermore, documentation was not provided to support if necessary changes were needed to be made to the policies.

Without properly assessing the privacy impact of each information system and maintaining a current privacy program, DFC may be unaware of what current privacy risk each system poses to the environment.

A recommendation addressing the PIAs was issued in the FY 2018 FISMA audit.[16] Since that recommendation is still open, we are not making a new recommendation. However, we are making a new recommendation to address the weakness with DFC's privacy policy and breach notification procedures.

> ***Recommendation 1:*** *We recommend the DFC Chief Information Officer review and update privacy policies and breach response procedures to accurately reflect the Corporation's operating environment.*

5. DFC Needs to Strengthen Personnel Onboarding Training Requirements

Cybersecurity Framework Security Function: *Protect*
FY 2020 FISMA IG Metric Domain: *Security Training*

NIST SP 800-53, Revision 4, security control Awareness and Training (AT)-2, states the following regarding security awareness training:

> The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
> a. As part of initial training for new users.

In addition, security control Planning (PL)-4, states the following regarding Rules of Behavior:

> The organization:

[16] Recommendation 1, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019).

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Controls were not adequate to ensure DFC personnel completed security and privacy training and signed required rules of behavior as part of new hire onboarding. Specifically, from a population of 173 new users, for a sample of 18 new users, we noted:

- Evidence of annual cyber security and privacy training, and rules of behavior completion was not provided for one user.
- Completion of cyber security and privacy training, and rules of behavior for one user was delayed for three weeks.

DFC management had not implemented a process to enforce training for individuals missing initial training or rules of behavior.

Without timely completion of initial training and signed rules of behavior, DFC management may not be able to ensure all users are aware of their information security responsibilities. This may result in users disclosing sensitive DFC information. Therefore, we are making the following recommendation.

> ***Recommendation 2:*** *We recommend the DFC Chief Information Officer implement a process to validate completion of rules of behavior and security and privacy awareness training prior to providing system access.*

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

Cybersecurity Framework Security Function: *Protect*
FY 2020 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 and/or the information system data. Therefore, we are making the following recommendation to address this weakness.

> ***Recommendation 3:*** *We recommend the DFC Chief Information Officer implement multifactor authentication for network access for privileged accounts.*

7. DFC Needs to Strengthen Remote Access Controls

Cybersecurity Framework Security Function: *Protect*
FY 2020 FISMA IG Metric Domain: *Identity and Access Management*

NIST SP 800-53, Revision 4, security control System and Communications Protection (SC)-10, states the following regarding network disconnect:

> The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

DFC's *NIST 800-53 Security Controls OPIC Organizational Parameters* document defines the requirement for virtual private network (VPN) session disconnect after 30 minutes of inactivity. However, DFC had configured its VPN to allow idle sessions to remain active for 2 hours before disconnecting.

DFC management was not aware that the extended idle timeout configuration setting for VPN access did not comply with DFC's defined security parameters.

Without proper security configurations settings for VPN access, DFC runs the risk of unauthorized access to its network through unlocked and unattended remote laptops. Therefore, CLA is making the following recommendation.

> ***Recommendation 4:*** *We recommend the DFC Chief Information Officer implement session disconnect for virtual private network connections to be compliance with DFC requirements.*

8. DFC Needs to Strengthen its Enterprise Architecture Strategy

Cybersecurity Framework Security Function: *Identify*
FY 2020 FISMA IG Metric Domain: *Risk Management*

NIST SP 800-53, Revision 4, security control Program Management (PM)-7, states the following regarding Enterprise Architecture (EA):

> The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, provides guidelines for applying the Risk Management Framework to information systems and organizations including the integration of security and privacy requirements into the enterprise architecture, system development lifecycle, acquisition processes and systems engineering processes.

OMB Circular A-130, *Managing Information as a Strategic Resource*, states the following regarding Enterprise Architecture:

> Agencies shall develop an EA that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. The agency's EA shall align to their IRM Strategic Plan. The EA should incorporate agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support missions or business functions. The EA should align business and technology resources to achieve strategic outcomes. The process of describing the current and future state of the agency, and laying out a plan for transitioning from the current state to the desired future state, helps agencies to eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among Government, industry, and citizens.

DFC's Office of the Chief Information Officer (OCIO) developed a strategic overview that describes the IT goals for the Corporation. However, the overview does not fully incorporate all requirements of an enterprise architecture strategy to include resulting risk to individuals, other organizations and the Nation. As a new agency, DFC is in the planning phase of the enterprise architecture strategy and therefore it was not complete during the audit.

The lack of risk management controls for enterprise architecture may increase the difficulty the Corporation has with managing the integration of security for its IT projects and assets.

A recommendation[17] addressing this finding was issued in the fiscal year 2019 FISMA Audit. Since that recommendation remains open, we are not making a new recommendation.

[17] Recommendation 3, *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-OPC-20-003-C, January 16, 2020).

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, DFC outlined its plans to address recommendations 1, 2, 3, and 4, but disagreed with part of recommendation 2. DFCs comments are included in their entirety in Appendix II.

Based on our evaluation of management's comments, we acknowledge DFC's management decisions on recommendations 1, 2, 3 and 4. Further, we consider recommendations 1 and 3 resolved, but open pending completion of planned activities, and recommendation 4 resolved, but open pending OIG's verification of the Agency's final actions.

In regards to recommendation 2, DFC management agreed with the recommendation to validate the completion of rules of behavior and security and privacy awareness training, but disagreed that the training be completed "prior to providing system access" because users require access to the network in order to take and track rules of behavior agreements and security awareness training completion. In response to the recommendation, DFC management said it had developed and implemented a process to validate that new users receive security awareness training timely. However, there has not been sufficient time to determine if management has implemented that process. Therefore, we consider recommendation 2 open-resolved pending OIG's verification of the Agency's final actions.

SCOPE AND METHODOLOGY

Scope

CLA conducted this performance audit in accordance with GAGAS. 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 the audit objective. CLA believes that the evidence obtained provides a reasonable basis for CLA's findings and conclusions based on the audit objective. The audit was designed to determine whether DFC implemented an effective[18] information security program.

The audit included tests of selected management, technical, and operational controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. CLA assessed DFC's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Media Protection
- Personnel Security
- Planning
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Services Acquisition
- Privacy Controls

For this audit, CLA reviewed selected controls related to the FY 2020 IG FISMA Reporting Metrics from all 3 information systems in DFC's systems inventory as of May 2020. In addition, we performed a vulnerability assessment of one of DFC's three systems. See Appendix III for a listing of the controls selected.

The audit also included a follow up on prior audit recommendations[19] to determine if DFC made progress in implementing the recommended improvements concerning its information security program. See Appendix IV for the status of prior year recommendations.

[18] For this audit, an effective information security program is defined as implementing certain security controls for selected information systems in support of FISMA.

[19] *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), *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018* (Audit Report No. A-OPC-19-006-C, January 30, 2019), and *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019* (Audit Report No. A-OPC-20-003-C, January 16, 2020).

Audit fieldwork covered DFC's headquarters located in Washington, DC, from May 7, 2020 to September 1, 2020. It covered the period from October 1, 2019, through September 1, 2020.

Methodology

To determine if DFC implemented an effective information security program, CLA conducted interviews with DFC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, CLA 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, CLA compared documents, such as DFC's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, CLA performed tests of system processes to determine the adequacy and effectiveness of those controls. Further, CLA reviewed the status of FISMA audit recommendations from fiscal year 2017, 2018, and 2019.[20]

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population. However, in cases where 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 the following guidance:

- OMB and DHS, *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*
- OMB Circular Number 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.*

[20] Ibid 19.

MANAGEMENT COMMENTS

MEMORANDUM December 2, 2020

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

FROM: Mark Rein
Chief Information Officer (CIO)
DFC – Office of Information Technology

Michael Goulding
Chief Information Security Officer (CISO)
DFC – Office of Information Technology

SUBJECT: DFC Comments on the Audit of the US International Development Finance Corporation's Fiscal Year 2020 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 2020 in Support of FISMA (A-DFC-21-00X-C)."

The Inspector General report contains four (4) new recommendations for corrective action. This memorandum provides DFC's management responses to these recommendations.

Recommendation No. 1: We recommend the DFC Chief Information Officer review and update privacy policies and breach response procedures to accurately reflect the Corporation's operating environment.

Management Response: The OIT/CISO agrees with the recommendation. Updated draft documents will be submitted for CIO/DCIO review (01/31/21). This response has been entered as a new line item **OIG-2020-01** in the DFC Plan of Action and Milestones (POA&M). DFC's Risk Rating: **Low**. Target due date: **3/31/21**.

Recommendation No. 2: We recommend the DFC Chief Information Officer implement a process to validate completion of rules of behavior and security and privacy awareness training prior to providing system access.

Management Response: The OIT/CISO agrees with the recommendation to validate the completion of rules of behavior and security and privacy awareness training. OIT/CISO disagrees with the recommendation training be completed "prior to providing system access". To validate the training completion, OIT/CISO updated the Cybersecurity Training Procedures to require better tracking of onboarding personnel using the Onboarding Training Tracker (OTT) spreadsheet. The OTT is a spreadsheet showing the scheduled EOD, the scheduled date of the OIT New Hire Orientation (NHO) and the final onboarding training completion date. The OTT also documents any discrepancies indicating why the account was not completed within the 5 days to include any coordination with the supervisor that lead to the account being disabled/reenabled. Final action was implemented on November 20, 2020.

With regards to the part of the recommendation that training be completed prior to system access, that part of the recommendation is unimplementable. The DFC training application cannot be accessed without a DFC user account.

Recommendation No. 3: We recommend the DFC Chief Information Officer implement multifactor authentication for network access for privileged accounts.

Management Response: The OIT/CISO agrees with recommendation and implementation of this recommendation will be in conjunction with the full transition of the DFC domain. This response has been entered as new line item **OIG-2020-02** in the DFC POA&M. DFC's Risk Rating: **Moderate**. Target due date: **04/01/21.**

Recommendation No. 4: We recommend the DFC Chief Information Officer implement session disconnect for virtual private network connections to be compliance with DFC requirements.

Management Response: The OIT/CISO agrees with this recommendation and has resolved the issue. The session disconnect for virtual private network connections was changed in compliance with DFC documentation (OPICNet SSP). The CR#16873 was approved by the Change Approval Board (CAB) and implemented 11/14/20.

/s/

SUMMARY OF CONTROLS TESTED

The following table identifies the controls selected for testing.

Control	Control Name	Number of Systems Tested
AC-1	Access Control Policy and Procedures	1
AC-2	Account Management	3
AC-8	System Use Notification	1
AC-17	Remote Access	1
AR-1	Governance and Privacy Program	1
AR-2	Privacy Impact and Risk Assessment	3
AR-4	Privacy Monitoring and Auditing	1
AR-5	Privacy Awareness Training	1
AT-1	Security Awareness and Training Policy and Procedures	1
AT-2	Security Awareness Training	1
AT-3	Role-based Security Training	1
AT-4	Security Training Records	1
CA-1	Security Assessment and Authorization Policies and Procedures	1
CA-2	Security Assessments	1
CA-3	System Interconnections	1
CA-5	Plan of Action and Milestones	1
CA-6	Security Authorization	3
CA-7	Continuous Monitoring	1
CM-1	Configuration Management Policies and Procedures	1
CM-2	Baseline Configuration	1
CM-3	Configuration Change Control	1
CM-6	Configuration Settings	1
CM-7	Least Functionality	1
CM-8	Information System Component Inventory	1
CM-9	Configuration Management Plan	1
CM-10	Software Usage Restrictions	1
CP-1	Contingency Planning Policy and Procedures	1
CP-2	Contingency Plan	1
CP-3	Contingency Training	1
CP-4	Contingency Plan Testing	1
CP-6	Alternate Storage Site	1
CP-7	Alternate Processing Site	1
CP-8	Telecommunication Services	1
CP-9	Information System Backup	1
IA-1	Identification and Authentication Policy and Procedures	1
IR-1	Incident Response Policies and Procedures	1
IR-4	Incident Handling	1
IR-6	Incident Reporting	1
IR-7	Incident Response Assistance	1

Control	Control Name	Number of Systems Tested
MP-3	Media Marking	1
MP-6	Media Sanitization	1
PL-2	System Security Plan	1
PL-4	Rules of Behavior	1
PL-8	Information Security Architecture	1
PM-5	Information System Inventory	1
PM-7	Enterprise Architecture	1
PM-8	Critical Infrastructure Plan	1
PM-9	Risk Management Strategy	1
PM-11	Mission/Business Process Definition	1
PS-1	Personnel Security Policy and Procedures	1
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	3
SA-3	System Development Life Cycle	1
SA-4	Acquisition Process	1
SA-8	Security Engineering Principles	1
SA-9	External Information System Services	2
SC-8	Transmission Confidentiality and Integrity	1
SC-28	Protection of Information at Rest	1
SE-2	Privacy Incident Response	1
SI-2	Flaw Remediation	1
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	1
SI-7	Software, Firmware, and Information Integrity	1
	Total Control Instances Tested	**75**

STATUS OF PRIOR YEAR RECOMMENDATIONS

The following tables provide the status of the FY 2017,[21] FY 2018,[22] and FY 2019[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

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.	Open	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
3	Document and implement a process to verify that patches are applied in a timely manner.	Open	Agree
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.	Open	Agree
7	Conduct (1) contingency training and (2) a test of the information system contingency plan in accordance with OPIC's policy.	Open	Agree

[21] *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).

[22] *OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018 (Audit Report No. A-OPC-19-006-C, January 30, 2019).*

23 OPIC Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2019 (Audit Report No. A-OPC-20-003-C, January 16, 2020).

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