# FY21 FISMA Report to Congress

U.S. International Development Finance Corporation

FY 2021

# FY21 FISMA Report to Congress

Pursuant to the Office of Management and Budget (OMB) Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, the United States International Development Finance Corporation (DFC) issues this report to Congress and the Government Accountability Office (GAO) to provide a detailed assessment of the adequacy and effectiveness of the Agency's information security policies, procedures, practices, and progress toward meeting Fiscal Year 2021 (FY21) government-wide targets in the Chief Information Officer (CIO) Federal Information Security Management Act (FISMA) metrics.

Throughout FY21, DFC continually strengthened its cybersecurity posture and defended the Agency against a vast array of threats. Bolstering its risk management program, DFC protected the sensitive data stored on its network and in its systems. While adversaries refined their sophisticated capabilities towards threatening the security of organizational information, DFC methodically invested in implementing defensive, preventative, and persevering techniques to reinforce and optimize the Agency's information security and privacy programs. Consistent with FISMA requirements, OMB policy, and applicable National Institute of Standards and Technology (NIST) guidelines, DFC has maintained its rigorous and effective information security policies, procedures, and practices.

DFC's mandatory and comprehensive cybersecurity training program has comprised part of this strategy. All users with elevated privileges have completed mandatory training, and the Agency continues to provide initial cybersecurity awareness and periodic refreshers of common attack vector types, for all employees and contractors.

Additionally, DFC began configuring, more granularly than before, automated monitoring of the network environment and changes therein and improved DFC's anti-phishing email capabilities (e.g., quarterly simulated phishing email trainings for all personnel and fine-tuning of mail flow rules to thwart phishing email attempts).

## Maturing Risk Management

DFC built upon its commitment to risk management through the Agency's Board of Directors Risk Committee, the Operational Risk Management Group, and the Agency's executive leadership. Combined with DFC's information security program, the Agency has maintained an improving governance structure and enterprise-wide risk management strategy for cybersecurity.

DFC's cybersecurity program has continued to find ways to mature and improve the overall security posture. In FY21, the United States Agency for International Development (USAID) Office of Inspector General (OIG) conducted a FISMA Audit for DFC that resulted in 4 findings with three (3) recommendations. As indicated in the USAID OIG's final report, the 3 recommendations are considered resolved by the USAID OIG, but open pending verification of completed activities. The USAID OIG also confirmed completion and agreed to the closure of ten (10) open recommendations from previous FISMA Audits.

For the third consecutive fiscal year, DFC achieved an Overall "Managing Risk" rating from the Department of Homeland Security (DHS) Risk Management Assessment (RMA) program.

*Table 1. FY21 DFC DHS RMA Rating*

| Framework | CIO Rating | OIG Rating |
|---|---|---|
| Identity | Managing Risk | Managed and Measurable |
| Protect | Managing Risk | Managed and Measurable |
| Detect | Managing Risk | Managed and Measurable |
| Respond | Managing Risk | Managed and Measurable |
| Recover | Managing Risk | Managed and Measurable |
| **Overall** | **Managing Risk** | |

In FY21, DFC increased OIG Metrics maturity level functions from FY20: Identity and Protect and Recover domains.

*Table 2. DFC Maintaining Maturity Levels*

| Cybersecurity Risk Management Function | FY20 | FY21 |
|---|---|---|
| **Identify** | Level 3 | Level 4 |
| **Protect** | Level 4 | Level 4 |
| **Detect** | Level 4 | Level 4 |
| **Respond** | Level 4 | Level 4 |
| **Recover** | Level 3 | Level 4 |
| **Overall** | MANAGING RISK | MANAGING RISK |

The following sections highlight key actions taken by DFC to improve the security posture, align with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, along with OMB guidance and DHS Binding Operational Directives (BOD)/Emergency Directives to achieve an Overall Managing Risk rating across the Cybersecurity Risk Management Functions.

## Identify

Throughout FY21, DFC worked to mature the Agency's asset inventory. DFC began implementation of automatic capabilities to identify 100% of its network assets and ensured that hardware and software assets are subject to monitoring processes through the deployment of tools such as Absolute and MS Defender for Endpoint. In addition, DFC has continued to invest in the modernization of the Agency's network infrastructure, including piloting tools to create private access to segment services through the network.

In FY21, one of DFC's most significant cybersecurity efforts was to improve the remediation of vulnerabilities and accelerate known exploitable vulnerability mitigation (BOD 22-01). As a result of that effort DFC was able to reduce exploitable vulnerability by over 50%.

During FY21, in direct response to the EO, DFC has achieved 100% Multifactor Authentication (MFA) for remote access through CITRIX and VPN and continues to improve efforts of PIV deployment.

## Protect

DFC is actively working in the function of "Protect" to strengthen controls in the areas of detection of unauthorized assets, and strong configuration of Agency assets. In order to support these activities, DFC invested in new infrastructure and technologies to materialize the Agency's vision of data protection at the endpoint, in transit, and at rest reporting 100% encryption. The Agency continues to implement a Trusted Internet Connection (TIC) and currently 100% of external traffic passes through a consolidated TIC.

DFC enhanced its security awareness training program by continuing to create and deliver quarterly anti-phishing email training campaigns for 100% of its users, then providing in-person additional phishing awareness training based on the user behavior data each campaign had generated.

In response to OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, DFC assessed the Investigative and Remediation capabilities to establish the Event Logging (EL) maturity baseline. DFC is currently at EL Tier 0 Not Effective. Logging requirements of highest criticality are partially met. DFC is 84% of meeting the EL1 due by 8/27/22.

In response to OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures*, DFC has taken steps to protect critical software through enhanced security measures. DFC has successfully completed Phase 1, identifying all Agency critical software and has initiated Phase 2 to deploy security measures. Currently fifteen (15) of the eighteen (18) (83%) discrepancies will be resolved once we complete the Personal Identity Verification (PIV) deployment.

DFC continues to fulfill the BOD 19-02 and has completed all required actions to ensure effective and timely remediation of critical and high vulnerabilities identified through Cyber Hygiene scanning. As a result, the Agency significantly reduced the likelihood that malicious actors could compromise DFC's network.

## Detect

Another significant cybersecurity enhancement during FY21 was network visibility. DFC has made improvements by upgrading the network Intrusion Detection System (IDS) and deployed a cloud-based Security Information and Event Management (SIEM) tool. Both projects increased visibility within the environment improving DFC monitoring and reporting capabilities.

Furthermore, DFC deployed the services of a third-party vendor to provide an assessment of the IT infrastructure. The DFC Office of Information Technology (OIT) team is working diligently to address the provided recommendations to improve the environment.

## Respond and Recover

DFC OIT directs resources to continuously monitor DFC networks and systems for signs of intrusion or unauthorized access and address system vulnerabilities. During FY21, DFC took significant steps to remove

unsupported software from the environment (100% Windows 7 and 90% Server 2008) and continues to make improvements.

DFC also responded to real-world events to remove SolarWinds and unsupported versions of MS Exchange from the environment.

During FY21, DFC reported seven (7) security incidents to US-CERT as required by FISMA. Most significantly, DFC did not detect any major incidents involving a breach of personally identifiable information (PII) or Agency business data.

Five (5) incidents were lost or stolen smartphones, one (1) was related to a phishing email, and one (1) was a false positive notification of a ransomware event. In each instance regarding the lost or stolen phones, the device was remotely sanitized and deactivated.

## Concluding Remarks

As part of DFC's ongoing technological growth across the enterprise, the Agency has increased investments in building out an entirely new infrastructure. These investments have been a continuous effort not only to provide even greater reliability among technical services for the Agency as a whole, but also to bolster DFC's cybersecurity resilience by updating and adding tools and monitoring capabilities. DFC further fortified its current and future information security stances with a combination of proactive program initiatives and continual adherence to overarching federal requirements.