Federal Information Security Modernization Act Report to Congress

Fiscal Year 2022

DFC U.S. International Development Finance Corporation

dfc.gov

Introduction

Pursuant to the Office of Management and Budget (OMB) Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, the U.S. International Development Finance Corporation (DFC) issues this report to Congress and the Government Accountability Office to provide a detailed assessment of the adequacy and effectiveness of the agency's information security policies, procedures, and practices, and to report DFC's performance against the government-wide Fiscal Year (FY) 2022 Federal Information Security Modernization Act (FISMA) target metrics.

Throughout FY 2022, DFC strengthened its cybersecurity posture and defended the agency against a vast array of threats. DFC bolstered its risk management program and protected the sensitive data stored on its network and in its systems. While adversaries refined their sophisticated capabilities to compromise organizational information, DFC methodically invested in implementing defensive, preventative, and persevering techniques to reinforce and optimize the agency's information security and privacy programs. DFC strengthened its information security policies, procedures, and practices consistent with FISMA requirements, OMB policy, and applicable National Institute of Standards and Technology guidelines.

DFC's FY 2022 Core Inspector General (IG) FISMA Metrics Report rated the Corporation on the five NIST Cybersecurity Framework security functions: Identify, Detect, Recover, Protect and Respond.

DFC received a lower overall maturity level rating of "Defined" on the five Cybersecurity Framework security functions, compared to FY 2021, where the agency received a higher overall maturity level rating of "Managed and Measurable."[1] This lower rating was attributed to the fact that this was the first year DFC was assessed after merging two domains/networks into one – OPICNet to DFCNet – which resulted in the need to decommission legacy systems. In addition, in FY 2022, DFC was measured on far fewer metrics than in FY 2021 and given a shorter time frame to respond to previously identified findings due to an earlier audit start date; therefore, the weighted impact of the IG's findings in FY 2022 had a much more significant impact in lowering the agency's overall maturity level rating than in years past, despite the agency's numerous information security accomplishments in FY 2022.

DFC received a "Defined" rating on three of the five security functions (Identify, Detect, and Recover), and an "Optimized" rating on the two remaining security functions (Protect and Respond). In FY 2022, DFC actively worked to remediate the weaknesses identified in the IG report on the three security functions in which it received a "Defined" rating and continued to monitor and strengthen the controls associated with the two security functions in which it received an "Optimized" rating.

Identify

DFC reached full multi-factor authentication implementation status by employing a combination of Personal Identity Verification (PIV) cards and hardware authentication devices for

[1] FY 2022 Core IG FISMA Metrics Evaluation Guide. Maturity level ratings are ranked in the following order, from least mature to most mature: 1) Ad Hoc; 2) Defined; 3) Consistently Implemented; 4) Managed and Measurable; 5) Optimized.

administrator accounts. This was applied to a zero trust architecture strategy to make access control enforcement as granular as possible and prevent unauthorized access to agency data services. DFC also implemented a cloud-based security solution that leverages cutting-edge artificial intelligence to identify advanced threats to the DFC network that can otherwise be extremely difficult to detect, such as insider threat and nation-state attacks. In addition, DFC entered its list of software assets into an electronic asset inventory and established an end-of-life dashboard to improve its ability to identify and remove unsupported software from its environment.

Protect

DFC completed the architecture for the Data Loss Prevention (DLP) tool and implemented it in November 2022. The DLP tool is an enterprise-wide network monitoring software that inspects outbound network communications, such as emails and their attachments. DFC is now able to detect and prevent the transmission of unencrypted sensitive data from leaving the DFC network, including but not limited to Social Security numbers, passport numbers, credit card numbers, and driver's license numbers.

Detect

DFC moved its Security Information and Event Management (SIEM) system to a cloud-based monitoring and search platform, which allows the Corporation to monitor, identify, analyze, and record information security incidents and events in real time with increased data streaming, search, visualization, and mobile device recognition capabilities. DFC also implemented a network security monitoring solution that allows it to collect and analyze live network traffic, which in turn gives it the opportunity to detect and respond to intruders in its network. This provides DFC with the ability to act before intruders manage to accomplish their mission, thereby preventing further damage to the network.

Respond

DFC began conducting penetration tests and quarterly tabletop exercises to simulate breaches. This helps to ensure that incident response personnel understand their roles and responsibilities during a breach and are well prepared to follow incident response procedures. DFC also updated its Incident Response Plan and Information Security Continuous Monitoring Plan to include a "lessons learned" analysis after each incident to inform personnel on how their responses can be improved for future incidents.

Recover

DFC completed a Business Impact Analysis (BIA) for a FISMA-reportable system[2] that was not previously completed. By maintaining an updated BIA for each FISMA-reportable system, DFC can prioritize its recovery operations in the event of a service-impacting incident. DFC also

[2] A FISMA-reportable system is an information system that supports the operations and assets of the agency, and FISMA requires the agency to implement an agency-wide program for information security for those systems. DFC has four FISMA-reportable systems: 1) DFCNet, 2) Credit Management System, 3) Insight, and 4) Oracle E-Business Suite.

completed a contingency plan for another FISMA-reportable system that was not previously completed. The contingency plan documents the processes for recovering systems as quickly and effectively as possible following a service disruption. Finally, DFC drafted master schedules to track reviews and updates to all system artifacts as part of its implementation of the Risk Management Framework for information systems requiring an authorization to operate.

Details on Information Security Incidents Reported to CISA

During FY 2022, DFC reported one information security incident to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System 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. The one information security incident was related to the sending of an unencrypted email containing home addresses, personal email addresses, and personal phone numbers of DFC employees, contractors, and their emergency contacts to a trusted outside contractor performing work on a database of emergency contacts that DFC was then using. The Office of Information Technology (OIT), led by the privacy and cybersecurity teams, conducted a risk of harm analysis based on the criteria established in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. This analysis included assessing the nature and sensitivity of the PII compromised, the likelihood of access and use of PII, and the type of breach that occurred. In the end, although OIT determined that the risk of harm to individuals was very low, the Senior Agency Official for Privacy sent a privacy breach notification to the employees and contractors affected by the breach to make them aware of what transpired.

Conclusion

As part of DFC's ongoing technological growth across the enterprise, DFC has increased its investments in building out its cybersecurity infrastructure. These investments support continuous efforts not only to provide even greater reliability among technical services for DFC as a whole but to bolster DFC's cybersecurity resilience by updating and adding tools and monitoring capabilities. In FY 2022, DFC responded to the identified weaknesses from the Core IG FISMA Metrics Report and ultimately used those findings as a growth opportunity to strengthen its current and future information security stance through the implementation of new program initiatives focused on tackling current cybersecurity challenges while adopting overarching Federal requirements.