USAID FISMA ANNUAL REPORTING UPDATE

FISCAL YEAR (FY) 2019 OVERVIEW

Overall, USAID's information security policies, procedures, and practices are strong and effective. The Department of Homeland Security (DHS) and the Office of Management and Budget (OMB) ranked USAID as *Managing Risk* for all functions in the Cybersecurity Risk Management Assessment (RMA), which places the Agency among the highest rated Federal departments and agencies for actively managing enterprise-wide cybersecurity risks.

This document provides a brief summary of what was previously reported for Quarters 1-3, an overview of Quarter 4 activities, a list of FY 2019 accomplishments and a description of next steps for FY 2020.

QUARTERS 1 - 3 (PREVIOUSLY REPORTED)

Quarters 1 and 2 were marked by notable improvements to the Agency's information security program. The results of the FY 2018 Federal Information Security Modernization Act (FISMA) audit were received, and the Office of the Chief Information Officer (OCIO) identified and prioritized resources to promptly address the auditor recommendations and unsatisfied controls. Despite the 35-day Federal Government shutdown, which resulted in the temporary suspension of workforce support for multiple programs, OCIO mitigated associated delays through the diligent work of personnel.

In Quarter 3, the USAID Inspector General (IG) Annual FISMA Audit began to assess the maturity of the Agency's information security program.[1] In Quarter 3, USAID received confirmation that the Agency achieved the highest possible score/rating for Cross Agency Priority (CAP) Goals[2] and for the Chief Information Officer (CIO) Metrics from OMB/DHS.[3]

QUARTER 4

In Quarter 4, the CIO, IG, and Senior Agency Official for Privacy (SAOP) delivered the FY 2019 FISMA Report to OMB, per Federal information and security and privacy management requirements defined in OMB Memorandum M-19-02[4]. The Agency also compiled its Annual FISMA Report to Congress.

FY 2019 ACCOMPLISHMENTS

By the end of FY 2019, M/CIO achieved several major milestones and objectives championed by USAID senior leadership, including high scores for metrics and audits, and made progress in several critical areas that serve to enhance the Agency's information security program.

METRICS AND AUDITS

The Agency achieved high scores for the following metrics and audits:

- **IG Metrics:** Achieved Maturity Level 4 and rated overall as having an *Effective*[5] information security program. Of the 59 metrics:
    - 33 percent advanced the Agency to the next maturity level, showing improvement.
    - 49 percent showed the Agency sustained the previously reported maturity level.
- **FISMA Audits:** Passed 144 of 156 security controls (92 percent) and received 33 percent fewer findings than FY 2018.
    - M/CIO successfully submitted all nine FY 2018 audit recommendations for closure well in advance of their target dates, with a 100-percent responsiveness rate.
- **CIO Metrics:** Received 10 out of 10 score for CAP Goals, and rated as *Managing Risk*.

[1] FISMA REQUIREMENTS MANDATE EACH AGENCY'S IG TO EVALUATE COMPLIANCE WITH CYBERSECURITY STANDARDS BASED ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800-53, REVISION 4.
[2] FROM THE PRESIDENTIAL MANAGEMENT AGENDA. USAID'S SCORE ON CYBER CAP GOALS WAS 10 OUT OF 10.
[3] OMB RISK MANAGEMENT ASSESSMENT (RMA) METHODOLOGY. USAID'S RATING WAS *MANAGING RISK*.
[4] OMB MEMORANDUM M-19-02, "FISCAL YEAR 2018-2019 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS PURPOSE".
[5] NIST SPECIAL PUBLICATION 800-53A, REVISION 4, "ASSESSING SECURITY AND PRIVACY CONTROLS IN FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS", DECEMBER 2014.

INFORMATION SECURITY PROGRAM ENHANCEMENTS

In FY 2019, USAID made significant progress in several critical areas:

- **Cybersecurity Tools:** The Agency deployed complementary cybersecurity tools that expanded the arsenal of resources used to strengthen the Agency's security posture to detect and prevent malicious malware attacks, phishing emails, and unauthorized data exfiltration. This includes threats to personally identifiable information (PII) and Advanced Persistent Threat (APT) activities. Based on the enhanced capabilities, USAID has seen a 48-percent increase in identified incidents reported to the US Computer Incident Readiness Team (US-CERT).
- **Information Security Continuous Monitoring (ISCM):** To meet the Agency's ISCM goals, OCIO built the M/CIO FISMA Continuous Monitoring (CONMON) executive dashboard. The dashboard provides senior management with an enhanced, interactive view of security weaknesses and prioritization of remediation efforts, all of which contribute to data-driven risk analysis, more effective execution of program goals, an evolving management approach, and better-informed risk decision-making across the Enterprise.
- **Continuous Diagnostics and Mitigation (CDM):** USAID also expanded its participation in the CDM project with the establishment of data feeds to the Department of Homeland Security (DHS) CDM dashboard, which increases visibility into USAID's security posture and enables the Agency to prioritize its response to risks accordingly.

FY 2020 NEXT STEPS

In the upcoming fiscal year, M/CIO will develop a strategy to improve USAID's FISMA program in key areas to enhance the Agency's ability to accomplish its goals, strengthen the cybersecurity posture of its information systems, and keep sensitive data and systems secure. Plans include the following:

- Satisfy and close all two FY 2019 audit findings early or on time.
- Improve information systems security posture and process, leading to maturing FISMA levels across the enterprise:
    - Set Agency goal of 20-percent or fewer findings from the FY 2020 FISMA Audit.
    - Expand cyber awareness communication and education campaign to cyber workforce through training.
- Leverage convergence of deployed complementary cyber tools across the enterprise to assist senior management to make risk-based decisions, resulting in:
    - Enhanced incident detection, containment, and recovery activities to provide quantifiable metrics for enhanced tracking.
    - Improved capability to identify and prevent high-risk behaviors that affect the Agency's security posture.
    - Heightened cybersecurity hygiene across the enterprise through continuous monitoring.