FISMA QUARTERLY REPORTING UPDATE

FY 2019 Q2 OVERVIEW

The first half of fiscal year (FY) 2019 marked notable improvements to the Agency's information security program. The results of the FY 2018 Federal Information Security Modernization Act (FISMA) audit were received in FY 2019 Q1, at which point the Office of the Chief Information Officer (OCIO) identified and prioritized resources to promptly address the auditor recommendations and unmet controls. Despite the 35-day Government shutdown, which resulted in the temporary suspension of direct hire staff and contractor resource support for multiple programs, OCIO mitigated associated delays through the hard work of key personnel to minimize impact to program schedules and prevent submission delays of Federal and FISMA reporting requirements.

The USAID FISMA Quarterly Reporting Update focuses on detailing progress between the annual FISMA audits and evaluation of the Inspector General (IG) metrics. The updates for FY 2019 Q2 are outlined below.

FISMA Roadmap Initiatives

OCIO developed a Continuous Monitoring (ConMon) Dashboard for internal use and to facilitate executive-level review of Agency risks in near real time. This granular management of FISMA-reportable information systems promotes enhanced management and oversight by the Authorizing Official (AO) to protect enterprise data and the Agency network from threats. Leveraging the compliance reporting per ADS 545, OCIO oversight supports risk mitigation and successful mission delivery for all Bureaus and Independent Offices (B/IOs).

OCIO presented the status of the IG ERM metrics and FY18 FISMA accomplishments to the Risk Management Council (RMC) on March 26, 2019. Discussions between OCIO, M/CFO, and the Agency's Chief Risk Officer (CRO) began in FY 2019 Q1 and remain ongoing to address the ERM-related IG metrics and outstanding action items. Presentations to the Executive Management Council on Risk and Internal Control (EMCRIC) and M Bureau senior staff to discuss ERM progress and

cybersecurity additions to the Agency Risk Profile (ARP) were conducted on June 25 and 26, 2019 (respectively).

M-19-02 FISMA Reporting Requirements

The Agency implemented the Department of Homeland Security (DHS) cyber threat intelligence feed in support of the FISMA requirements and action items outlined in M-19-02. The development and implementation of this solution leverage threat intelligence to identify deficiencies in the Agency's security capability coverage against any adversarial activity. OCIO continues to fine-tune this requirement with Agency-specific data and training to security operations center (SOC) personnel.

FY 2019 Q3/Q4 NEXT STEPS

FISMA Audit Preparation

As required by FISMA, the annual FY 2019 FISMA audit kicked off in FY 2019 Q3. The overarching FISMA audit objective is to determine whether USAID has implemented an effective information security program. An effective information security program is defined as implementing select security controls for selected information systems in support of FISMA as outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

The audit represents a collaborative effort across the Office of Inspector General, Information Technology Audit Division (OIG) and OCIO. Planned activities in FY 2019 Q3 and Q4 include:

- Interview key personnel and stakeholders;
- Review information on system control policies, procedures, and objectives;
- Perform tests on selected system controls;
- Evaluate the progress towards resolving known information security program weaknesses; and
- Discuss potential findings with OIG and then with management throughout the audit process to ensure potential issues are properly vetted.

USAID continues to target a Level 4 maturity (*effective* information security program) for all core functions in the FY 2019 FISMA audit, which will conclude at the end of the fiscal year in FY 2019 Q4.

OCIO will communicate the status of the FY 2019 FISMA audit to key stakeholders, system owners, and Information System Security Officers (ISSOs), as appropriate. OCIO will leverage lessons learned from previous quarters and continue to build the Agency's security posture and maturity level through ConMon activities and active management of cybersecurity risk to the enterprise.