USAID FISMA QUARTERLY REPORTING UPDATE

FY 2019 Q3 OVERVIEW

The annual FY 2019 Federal Information Security Modernization Act (FISMA) audit is underway with the USAID Office of Inspector General (OIG) to assess the maturity of the Agency's information security program. 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 800-53, Revision 4. The FY 2019 Chief Information Officer (CIO), Inspector General (IG), and Senior Agency Official for Privacy (SAOP) FISMA reporting is due to the Office of Management and Budget (OMB) by October 31, 2019, per the federal information and security and privacy management requirements defined in M-19-02.

Binding Operational Directive (BOD) 19-02, issued on April 29, 2019, states Agencies must remediate: 1) critical vulnerabilities within 15 calendar days of initial detection; and 2) high vulnerabilities within 30 calendar days of initial detection. To ensure compliance, the Office of the Chief Information Officer (M/CIO) Computer Security Incident Response Team (CSIRT) reviews any critical or high vulnerabilities and associated action items in daily scrum calls to expedite remediation and promote real-time collaboration among the CSIRT and Information Technology Operations (ITO) Division workstreams.

The FY 2019 Q3 updates are highlighted below.

FISMA ROADMAP INITIATIVES

In conjunction with the Office of Security (SEC), M/CIO rolled out the annual cybersecurity and privacy training on May 1, 2019 in accordance with the training requirements outlined in USAID's Automated Directives System (ADS) 545. Training was released and communicated with SEC in a joint effort and includes role-based training for select individuals dependent on their role and function (including annual training for the SEC administrator). FISMA requires mandatory security awareness training for all Agency personnel, including contractors and other users of information systems that support the information assets and operations of the Agency.

Discussions between the Chief Risk Officer (CRO), M/CIO, and Enterprise Risk Management (ERM) teams are ongoing to update the Agency Risk Profile (ARP) as needed and ensure the timely remediation of ERM-related IG metric action items. This includes, but is not limited to, the timely and consistent communication of risks to all internal and external stakeholders with a need-to-know, as well as the continuous evaluation of the effectiveness of the Agency's enterprise risk management strategy and program.

M-19-02 FISMA REPORTING REQUIREMENTS

The Agency submitted the Security Operations Center (SOC) Maturation Plan in accordance with the requirements outlined in M-19-02. OMB and DHS will work with Agencies to assess and enhance SOC maturity and streamline security operations across the enterprise, designed to improve and centralize visibility of network activity. The submission of the SOC Maturation Plan in May 2019 represents the first step in a cross-Agency effort to review the current and future SOC capabilities across the federal landscape to best address the delivery of future SOC services by DHS.

FY 2019 Q4 NEXT STEPS

ANNUAL FISMA AUDIT

M/CIO continues to collaborate with OIG to compile the requested documentation and artifacts to support the testing of security controls for selected FISMA-reportable information systems, as outlined in the NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The FISMA package due to OMB by no later than October 31, 2019 (per the M-19-02), comprises the following:

1. USAID Transmittal Letter to OMB
2. Assistant Administrator for Management (AA/M) Clearance Letter
3. SAOP Annual Reports
4. SAOP Metrics
5. OIG FY19 Audit Report
6. CIO FY19 Annual Metrics

OMB and DHS use these artifacts to compile the Annual FISMA Report to Congress and use the CIO and IG reporting to develop agency-specific or government-wide risk management assessments as part of an ongoing effort in support of Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The Agency target of a Level 4 maturity, an indicator of having an *effective* information security program, is still in place for all five functions aligned with the NIST cybersecurity framework (NSF): *Identify, Protect, Detect, Respond,* and *Recover*. M/CIO will continue to communicate the status of the FY 2019 FISMA audit and request supporting documentation from key stakeholders as appropriate.