USAID FISMA ANNUAL REPORTING UPDATE

FISCAL YEAR (FY) 2020 OVERVIEW

FY 2020 tested USAID's resilience, requiring the Agency to commit to rapid changes in its information technology investments. As one of the first Federal government agencies to adopt cloud computing nearly a decade ago, USAID's decision proved prescient when the Coronavirus Disease 2019 (COVID-19) pandemic required the Agency to pivot its workforce to wide-scale telework in a matter of hours. The workforce was able to leverage all of the Agency's tools and computing capabilities despite the challenges of an increased number of cyber attacks resulting from increased telework. The Agency was able to reduce cybersecurity risks to the network, data, and workforce in more than 80 countries around the world through collaboration across multiple Bureaus and Independent Offices, ensuring mission delivery.

FY 2020 ACCOMPLISHMENTS

The Agency achieved a major milestone: the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB) ranked USAID as "Managing Risk" for all enterprise-wide functions in the Cybersecurity Risk Management Assessment, which placed the Agency in the top percentile of rated Federal departments and agencies. USAID conducted the following activities that contributed to its FY

2020 successes: (1) identified deficiencies and strengths for continuous improvement by applying the Cyber Security Framework (CSF) to the enterprise environment via ongoing self-assessments against Federal Information Security Modernization Act of 2014 (FISMA) maturity level standards; (2) demonstrated progress toward meeting or surpassing OMB and DHS cybersecurity standards through the advanced collection and analysis of Agency FISMA metrics, in response to the President's Management Agenda (PMA); (3) rigorously evaluated the existing information security program, including the information technology (IT) privacy program, against National Institute of Standards and Technology (NIST) security controls, applicable laws, regulations, and USAID policies; and (4) worked to improve the Agency's cybersecurity tools, information security continuous monitoring (ISCM) activities, and continuous diagnostics and mitigation (CDM) pilot program, which are all priorities for FY 2021.

In Quarter 4 (Q4), USAID moved forward with the deployment of next generation firewalls to overseas Missions and implemented remote IT patching to ensure the security of network and system logins. Additionally, USAID completed a targeted assessment of security controls on high value assets (HVAs). The Agency also conducted a successful wide-scale phishing exercise to increase awareness of and vigilance against malicious emails. Finally, the Agency continued to develop a transition plan and timeline for updating the Agency's information security and privacy programs to reflect the revised standards in NIST SP 800-53 Revision 5, *Security and Privacy Controls*, including alignment of Agency policy and use of IT tools.

FY 2021 NEXT STEPS

M/CIO will take the following actions in FY 2021 to improve the Agency's information security posture:

- Launch a pilot cybersecurity compliance tool to support the Enterprise Risk Management (ERM) program.
- Work with other Agency bureaus to fulfill the following Agency Risk Profile (ARP) tasks:
  - Implementation of an Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) program (in part to address National Defense Authorization Act [NDAA] Section 889 requirements)
  - Facilitation of secure worldwide access to government-furnished equipment (GFE) and Internet for all categories of staff
- Extend training and awareness activities.
- Expand the CDM pilot across the global workforce in conjunction with DHS.
- Participate in the annual FISMA audit on identified IT systems.
- Comply with FISMA reporting guidelines outlined in OMB memorandum M-21-02[1].

[1] Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements