USAID
FROM THE AMERICAN PEOPLE

USAID FISMA QUARTERLY REPORTING UPDATE

FY 2020 Q2 OVERVIEW

In Quarter 2 (Q2), the spread of the Coronavirus Disease 2019 (COVID-19) led to a leadership decision to enact wide-scale telework so that the USAID workforce could stay safely at home while continuing to remain productive. Agency-wide telework introduced unique information security challenges and the Bureau for Management, Office of the Chief Information Officer (M/CIO) was able to overcome them and continue to provide strong and consistent information technology (IT) services, operations, and robust cyber protection to the Agency's workforce worldwide.

In Q2, despite the challenges associated with Agency-wide telework, M/CIO made progress in many projects and tasks, including:

1. Providing support and coordination for the Federal Information Security Modernization Act (FISMA) audit through the end of FY 2020.
2. Completing the Office of the Inspector General (OIG) Metrics Self-Assessment and continuing to fill in the gaps to help improve USAID's FISMA levels.
3. Closing the last of seven FY 2019 FISMA Audit recommendations by the end of FY 2020 or sooner.
4. Completing the Privacy Common Controls Assessment and Catalog.

5. Proceeding with Cyberscope reporting tasks despite the pause instituted by the Office of Management and Budget (OMB) in M-20-21[1]. The quantitative metrics continued to show a positive trend.
6. Sending out 9 Agency Notices pertaining to cybersecurity and 11 Cyber Awareness Notices / Cyber Security Alerts since the Agency-invoked telework began.

FY 2020 NEXT STEPS

Leading into Quarter 3 (Q3), M/CIO plans to focus on the following task areas:

1. Ensure Agency processes, tools, and technologies continue to work in sync and execute with precision to maintain the strong trend in Cyberscope CIO quantitative metrics reporting.
2. Work closely with OIG auditors and remediate any preliminary findings before issuance of the FISMA Audit Annual Report.
3. Continue to educate the workforce about cybersecurity issues and concerns via weekly Agency Notices, Cyber Awareness Alerts, and CyberSecurity Notices.
4. Develop a plan to transition to the NIST SP 800-53[2] Revision 5 Security and Privacy Controls.
5. Assure the workforce completes Annual Cybersecurity and Privacy Training by June 15, 2020 or sooner.
6. Continue to work closely with the Office of the Chief Financial Officer (M/CFO) and other stakeholders in support of Enterprise Risk Management (ERM). An important next step is to finalize a procurement strategy for a Governance, Risk, and Compliance (GRC) tool, followed by a phased pilot approach to implementation.

In summary, M/CIO has overcome significant challenges in Q2 as the Agency has adjusted to full telework in response to COVID-19. M/CIO staff continue to work around the clock to ensure that the workforce has all necessary IT services and protections to continue executing their tasks and delivering on the Agency's mission.

[1] Office of Management and Budget (OMB) Memorandum M-20-21, Implementation Guidance for Supplemental Funding Provided in Response to the Coronavirus Disease 2019 (COVID-19)

[2] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations