OFFICE OF INSPECTOR GENERAL
U.S. Agency for International Development

MANAGEMENT ADVISORY

DATE: May 8, 2025

TO: Leo J. Ruth
Acting Director
USAID/Office of Security

Jason Gray
Chief Information Officer
USAID/Bureau for Management/Office of the Chief Information Officer

FROM: Gabriele Tonsil /s/
Acting Assistant Inspector General for Audits, Inspections, and Evaluations

SUBJECT: Vulnerabilities at Two Overseas Missions Raise Serious Concerns About the Safety of Americans and Government Assets (A-000-25-001-A)

The USAID Office of Inspector General (OIG) is alerting you to security concerns at two USAID missions—one of which is a high-threat mission.[1] We visited the missions in February 2025 as part of an annual audit required under the Federal Information Security Modernization Act of 2014. One mission is collocated with a U.S. embassy; the other mission is not. During the visits, we observed vulnerabilities to physical access security at both missions. For the mission collocated with a U.S. embassy, we identified concerns with entry into USAID's facility; and at both missions, we identified concerns with access to restricted information technology (IT) areas.[2] We acknowledge that USAID is in the process of winding down its operations overseas. However, as long as the Agency maintains a presence abroad, such vulnerabilities will put Americans and Agency IT systems at risk and, therefore, warrant the attention of Agency officials. In finalizing the advisory, we considered your comments on the draft and included them in their entirety in the appendix.

Vulnerabilities at the USAID Mission Collocated With a U.S. Embassy

We identified two vulnerabilities at the mission collocated with a U.S. embassy. First, we observed that embassy security guards conducted visual checks of badges before granting entry

[1] According to the USAID Office of Security's website, characteristics of a high-threat mission include being located in a country with high levels of terrorism and political violence and a host government that is unable or unwilling to provide adequate security.
[2] Our observations in this management advisory are not part of an ongoing audit, evaluation, or inspection.

to both the embassy compound and the USAID facility within the compound. Visual checks can verify that the individual matches the photo on the badge and the date on the badge has not yet expired. However, a visual check cannot verify that the individual is still cleared for access to the facility. The embassy security guards did not review access lists to confirm whether individuals were still Agency employees. In addition, individuals were not required to swipe their badges to confirm whether they were still employees before they were granted access to the facility.

Second, mission officials told us that the lock combinations for restricted IT areas—housing telephone lines, servers, and IT equipment—are not changed immediately after personnel depart the mission. According to USAID's Automated Directives System (ADS), Agency staff must change lock combinations when individuals with that information are transferred or terminated.[3] Because the mission is located on a U.S. embassy compound, mission officials said they relied on the physical access controls from the Department of State and did not have written procedures specific to the mission to address this issue.[4] Instead, mission officials said State informs them when the combinations are changed, and they are not aware of and could not provide State's criteria for making the changes. However, officials from USAID's Office of Security located in Washington, DC, told us that the combinations are changed quarterly, but any written procedures would need to come from State.

We requested documentation regarding the mission's physical access procedures. We also asked if USAID and State have an agreement outlining State's responsibilities for changing the lock combinations. Mission officials did not provide requested documentation. Immediately following our site visit, many USAID staff were placed on administrative leave, thereby limiting our ability to follow up on this issue. In addition, because the ADS was no longer available after our visits, we could not review it to identify other Agency-specific policies for physical security and evaluate whether those policies contributed to the vulnerabilities we identified at the mission.

Vulnerabilities at the USAID Mission Separate From a U.S. Embassy

We also identified several vulnerabilities at the mission that was not collocated with a U.S. embassy. We found that the mission did not maintain a complete list of individuals authorized to access sensitive areas—including a computer lab and 10 closets that have mission-critical servers and routers on the Agency's network and cables—and could not provide evidence that the access list was periodically reviewed. Also, mission personnel did not maintain a list of individuals authorized to access the server room. [5] Moreover, at the time of our visit, the keys to the closets were left on a table in the computer lab rather than locked in a desk or cabinet.

[3] USAID, ADS, Chapter 545, Section 545.3.12.3, "Physical Access Control (PE-3) and Visitor Access Records (PE- 8)," partial revision, January 16, 2025. We accessed this directive on January 22, 2025.
[4] According to a USAID Office of Security official, all U.S. embassies are controlled by the Department of State.
[5] The National Institute of Standards and Technology defines a server as a "computer or device on a network" that may manage files, printers, network traffic, and database queries.

According to the ADS, USAID must maintain a list of individuals approved to access facilities that contain systems such as the Agency's network, review that list daily, and secure keys.[6]

In addition, the mission was unable to determine who accessed the computer lab and closets. Specifically, we found that the mission did not have a logging mechanism to track and monitor access to the computer lab and closets. Also, the mission did not establish a mechanism to immediately report suspicious or unauthorized access or have written procedures for responding to physical access breaches in sensitive areas. According to the ADS, USAID must monitor access to facilities that contain systems and, when anomalies occur, work with the Agency's incident response capability.[7] Mission officials explained that adherence to these ADS procedures did not occur because staff were not adequately trained on their job responsibilities for physical security.

IT systems within USAID missions, both collocated with and separate from U.S. embassies, maintain sensitive information, such as personnel records, travel plans, financial information, and information critical to the Agency's programmatic oversight. With unauthorized access, nefarious actors, such as terrorists or hackers, could: (1) alter server information, install clandestine surveillance equipment, or otherwise compromise equipment to jeopardize the safety and security of U.S. government information; (2) exploit American citizen's personally identifiable information to steal identities, leading to information loss to the U.S. government and individuals; and (3) steal IT equipment, which could result in exorbitant and wasteful replacement costs. Furthermore, the trust that the American public and foreign nations have in the U.S. government could be lost because of unauthorized access to U.S. facilities and IT systems.

While we are not making recommendations, we strongly urge USAID officials to verify that individuals are authorized to access all Agency facilities and sensitive IT areas abroad. This is critical as long as the Agency has a presence abroad.

We provided our draft management advisory to USAID on April 10, 2025, and received the Agency's response, on April 23, 2025, which is included as the appendix to this advisory.

USAID management said they partially agreed with the vulnerabilities identified though they did not identify any disagreement with our observations. They also provided technical comments, which we addressed as appropriate.

USAID stated in its comments that the OIG did not meet with State Regional Security Officers who could have provided additional context about the security procedures at the missions. We acknowledge that those officers oversee and manage overseas physical security. However, we did not meet with them because they were not within the scope of the Federal Information Security Modernization Act of 2014 audit, which was the purpose of the site visits. Nonetheless, OIG has a responsibility to report its observations to USAID.

[6] ADS 545.3.12.2, "Physical Access Authorizations (PE-2)" and 545.3.12.3, "Physical Access Control (PE-3) and Visitor Access Records (PE-8)," partial revision, January 16, 2025.
[7] ADS 545.3.12.5, "Monitoring Physical Access (PE-6)" and 545.3.9.4, "Incident Handling (IR-4)/ Incident Monitoring (IR-5)," partial revision, January 16, 2025.

USAID partially agreed with the vulnerabilities identified at the USAID mission collocated with a U.S. embassy and identified challenges specific to changing lock combinations. USAID also explained that the vulnerabilities are mitigated because staff who leave the Agency must return their badges. However, USAID has a long-standing weakness in staff not completing the separation process, which includes returning their badge.[8] As a result, we believe that attention to this issue is warranted given that USAID is winding down these missions.

USAID partially agreed with the vulnerabilities identified at the USAID mission separate from a U.S. embassy, explaining that the risk of inappropriate access to IT space is low. While mitigation measures should be commensurate with the level of risk, USAID should still take appropriate actions to safeguard sensitive IT areas as it winds down these missions.

We prepared this management advisory in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspectors General* based on work completed from February 2–6, 2025. We conducted a site visit to one USAID mission collocated with a U.S. embassy from February 3–6, 2025, and another that was not collocated with an embassy from February 2–6, 2025. During the visits, we interviewed USAID personnel and observed facility access practices. We also requested and received information from USAID's Office of Security personnel located in Washington, DC, after those visits. In addition, we reviewed portions of the ADS, specifically Chapter 545 on policies and standards for physical access controls to information systems. After our visits, we were no longer able access other ADS chapters to identify other Agency-specific policies for physical access and evaluate whether those policies contributed to the vulnerabilities we identified.

We appreciate the assistance provided to our staff during our site visits.

[8] USAID OIG, *FISMA: USAID Implemented an Effective Information Security Program for Fiscal Year 2024 but Longstanding Weaknesses Persist* (A-000-24-005-C), September 19, 2024.

Appendix. Agency Comments

MEMORANDUM

TO: Gabriele Tonsil
Acting Assistant Inspector General for Audits, Inspections, and Evaluations

FROM: Jason Gray, Chief Information Officer /s/
USAID/Office of the Chief Information Officer

Leo J. Ruth, Acting Director /s/
USAID/ Office of Security

DATE: April 15, 2025

SUBJECT: Management Comments to Respond to the Office of Inspector General's (OIG) Draft Management Advisory titled, *Vulnerabilities at Two Overseas Missions Raise Serious Concerns About the Safety of Americans and Government Assets (A-000-25-001-A)*

The U.S. Agency for International Development (USAID) would like to thank the Office of Inspector General (OIG) for the opportunity to provide comments on the subject draft report. The Agency agrees in principle with the recommendations.

USAID is in the middle of shutting down as an independent organization with the end state to transition critical business operations to the Department of State (DoS). This involves closing our USAID locations overseas as part of the Agency's drawdown effort. With this end state in mind and with minimal resources to address or act on the evaluations stated in the report USAID provides following comments and will not be taking direct action on the recommendations.

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE DRAFT MANAGEMENT ADVISORY RELEASED BY THE USAID OFFICE OF THE INSPECTOR GENERAL (OIG) TITLED,Vulnerabilities at Two Overseas Missions Raise Serious Concerns About the Safety of Americans and Government Assets (A-000-25-001-A)

Please find below the management comments from the U.S. Agency for International Development (USAID) on the draft report produced by the Office of the USAID Inspector General (OIG), which contains general observations and feedback and for 2 areas:

Overall Management Comments: USAID acknowledges the observations identified by the OIG; however, there is no mention of the OIG team meeting with the Regional Security Officer (RSO) during either inspection. Interaction with the RSO in both locations would provide additional context to the security procedures noted during the inspection. More importantly, OIG staff would understand the areas of responsibility for Washington-based offices. The RSO oversees and manages all security programs for all USAID facilities regardless of whether a Mission is collocated with a U.S. Embassy or away from the Embassy. This includes those related to personnel protection, facility security, access control, and information protection.

Vulnerabilities at the USAID Mission Collocated With a U.S. Embassy

- **Management Comments:** USAID partially agrees with the evaluation of the physical security protocols in that the security check could be improved. Given that the location is collocated with the Embassy, the Department of State governs and manages the physical security protocols and procedures. Additionally, it was noted that the security guards only did a visual check of the badge and cannot verify that the individual is still cleared for access. This is mitigated by the fact that employees who separate must return their physical badge. A former employee can not visit or attempt to come back onto the compound without an active and current badge.

- **Management Comments:** USAID partially agrees with the evaluation on changes to the lock combination for restricted IT areas. Due to USAID's reliance on the Embassy for certain building functions, it is difficult to fully enforce changes such as lock combinations for restricted IT areas. The risk is low with only a few IT staff who have knowledge of the combination.

Vulnerabilities at the USAID Mission Separate From a U.S. Embassy

- **Management Comments:** USAID partially agrees with the evaluation on maintaining a control access list for physical spaces and ensuring better safeguarding for keys to various IT closets. However, the risk is low as there are limited staff who have access to the IT area, which presents several layers of entry and access controls requiring knowledge of a cipher PIN or a physical key to access.

- **Management Comments:** USAID partially agrees with the evaluation on the safeguard of data and information in the office space and its risk. As an example, the potential risk of stolen IT equipment (e.g., laptops) is low and mitigated by procedures USAID has in place for reporting stolen items and the ability to remotely wipe devices to ensure the removal of USAID data. Additionally, there are no staff or unauthorized individuals permitted in the facility without proper clearance and access credentials.