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

MANAGEMENT ADVISORY

DATE: May 13, 2025

TO: Kelly Larkins
Acting Chief of Travel and Transportation
USAID/Bureau for Management/Office of Management Services/Travel and Transportation Division

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: Information Security: Weaknesses in USAID's Management of Travel System Account Closures Highlight Concerns About Protecting Travelers and Sensitive Information (Report No. A-000-25-002-M)

The USAID Office of Inspector General (OIG) is alerting you to concerns with USAID's End-to-End Travel system (known as E2). In September 2024, OIG reported on a long-standing weakness related to USAID's offboarding of employees. Specifically, the Agency was not disabling user accounts within 24 hours of employees' separation dates, as required by USAID policy.[1] Controlling access to USAID systems is critical for protecting sensitive information from unauthorized access, modification, and disclosure.

We initiated an evaluation to further understand USAID's controls for disabling access to the E2 travel system following employee departures. Our objective was to assess the extent to which USAID disabled users' E2 accounts in accordance with Agency policy.[2] We reviewed E2 data from December 1, 2023, through November 30, 2024. We found that USAID did not disable accounts for 76 percent of users (137 of 178) within 24 hours of their separation, as required. As a result, the Agency faces the risk that unauthorized users will access sensitive travel plans, personally identifiable information, and credit card numbers of current or former

[1] 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.

[2] We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspectors General*. See Appendix A for a discussion of our scope and methodology.

employees. We made five recommendations to strengthen USAID's controls around its sensitive travel data.

In finalizing this advisory, we considered your comments on the draft and included them in their entirety in Appendix B. Based on our review of the comments and subsequent correspondence, we consider Recommendations 1 and 2 open and resolved pending further actions; Recommendations 3 and 4 open and unresolved; and Recommendation 5 closed. Please provide evidence of final action for Recommendations 1 and 2 to the Audit Performance and Compliance Division.

Background

Like other Federal agencies, USAID manages employee travel using E2, an internet-based travel management system located outside of the Agency's firewalled network. [3] Employees can use the system to create, submit, and approve travel authorizations and vouchers and book reservations, including flights, hotels, and rental cars. From December 1, 2023, through November 30, 2024, USAID processed 43,282 vouchers in E2 with a total value of over $132.9 million.

Within USAID's Bureau for Management, the Office of Management Services' Travel and Transportation Division (TTD) is responsible for the Agency's worldwide travel program. TTD establishes Agency-wide policies for travel and transportation and manages travel for U.S. direct hire employees and personal service contractors (collectively referred to as employees hereafter).[4] In addition, USAID's system owner for E2 is in TTD and is responsible for ensuring that appropriate security controls are implemented and operating as intended.[5] The system owner designated system administrators, who are located throughout the Agency, as the account managers, giving them responsibilities such as account creation and deletion.

USAID's Office of the Chief Information Officer, also within the Bureau for Management, is responsible for Automated Directives System (ADS), Chapter 545, *Information Systems Security*.[6] ADS 545 defines the security policies for all information systems owned by or operated on behalf of USAID. For example, ADS 545 establishes requirements for disabling user accounts in

[3] National Institute of Standards and Technology (NIST) Special Publication 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems,* October 2015, defined a firewall as a system "designed to block unauthorized access while permitting outward communication."

[4] According to Federal Acquisition Regulation Part 37.104, a personal service contract creates an employer-employee relationship "between the government and the contractor's personnel."

[5] NIST, Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations*, December 2018.

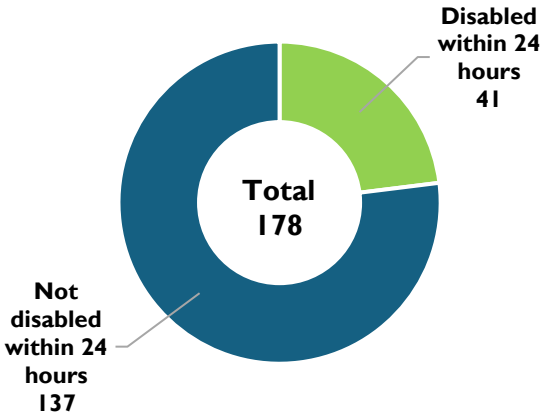
[6] USAID, Automated Directives System (ADS), Chapter 545, partially revised January 16, 2025.

Agency systems. Specifically, the Agency must disable system access within 24 hours of an employee's separation.[7]

USAID Did Not Consistently Disable Access to the Travel System as Required by Agency Policy

We found that from December 2023 through November 2024, USAID did not disable accounts for 76 percent of users (137 of 178) within 24 hours of their separation from the Agency as required by ADS 545 (see Figure 1).[8] This included 77 accounts that USAID disabled 64 to 351 days after the user's separation, and another 33 accounts for which USAID did not have a record of disabling (see Figure 2).[9]

Figure 1. E2 User Accounts Disabled Within 24 Hours of Separation Date, as of January 13, 2025



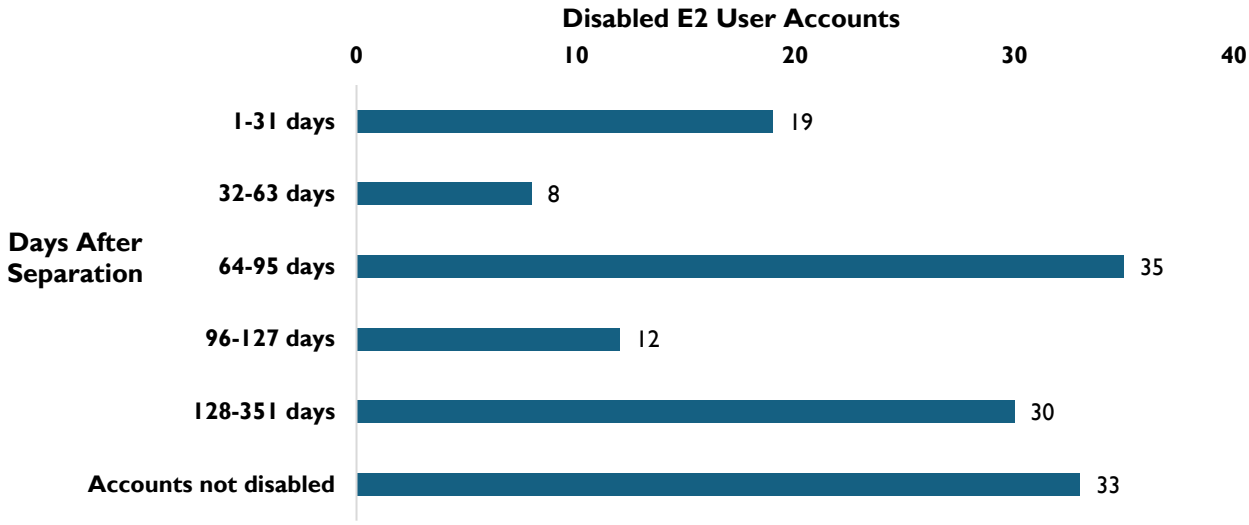
Source: OIG-generated graph from E2 and staffing pattern data from December 2023 through November 2024, as of January 13, 2025.

[7] ADS 545.3.14.4, *Personnel Termination (PS-4)*.

[8] ADS 545.3.14.4, *Personnel Termination (PS-4)*.

[9] We reviewed 26 separated OIG users, 4 of whom had E2 accounts. Of these four accounts, three were not disabled within 24 hours of the user's separation date. However, those three accounts were disabled as of the date of our analysis, January 13, 2025.

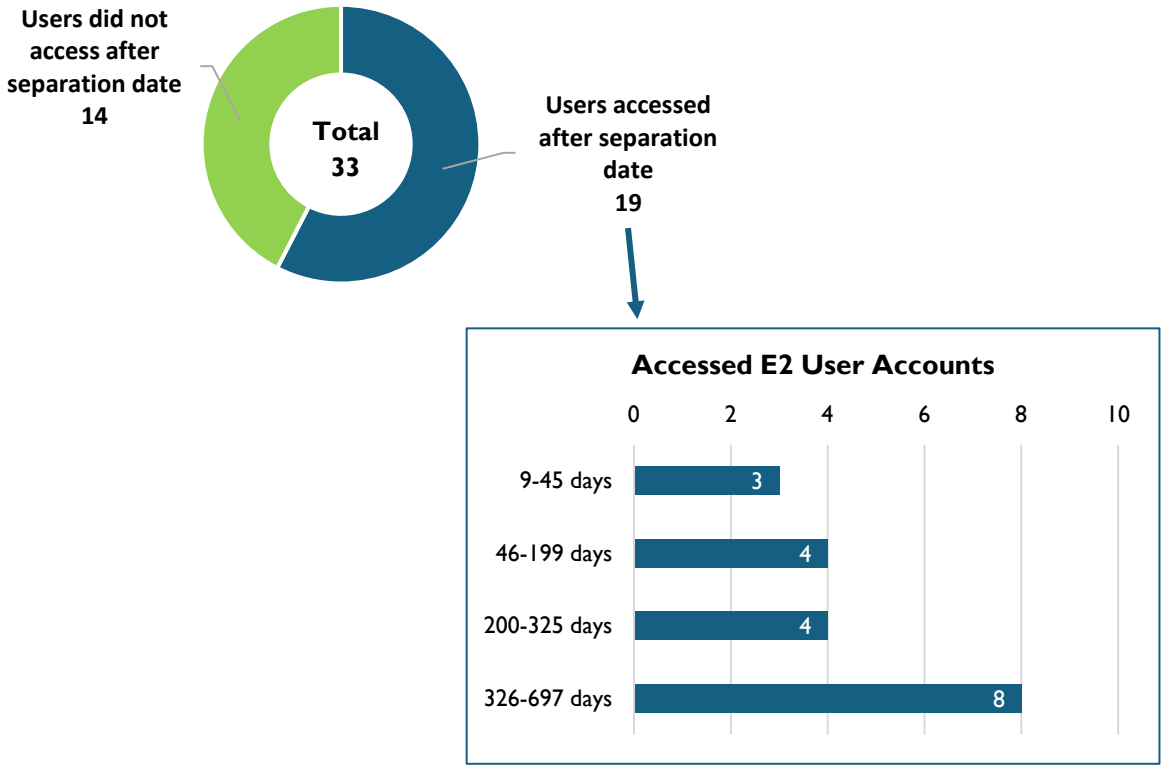
Figure 2. E2 User Accounts Disabled After Separation Date, as of January 13, 2025



Source: OIG-generated graph from E2 and staffing pattern data from December 2023 through November 2024, as of January 13, 2025.

For the accounts that USAID did not disable, we found that almost 57 percent of users (19 of 33) accessed E2 after their separation dates (see Figure 3). This included eight users who accessed the system more than 325 days after separating from the Agency.

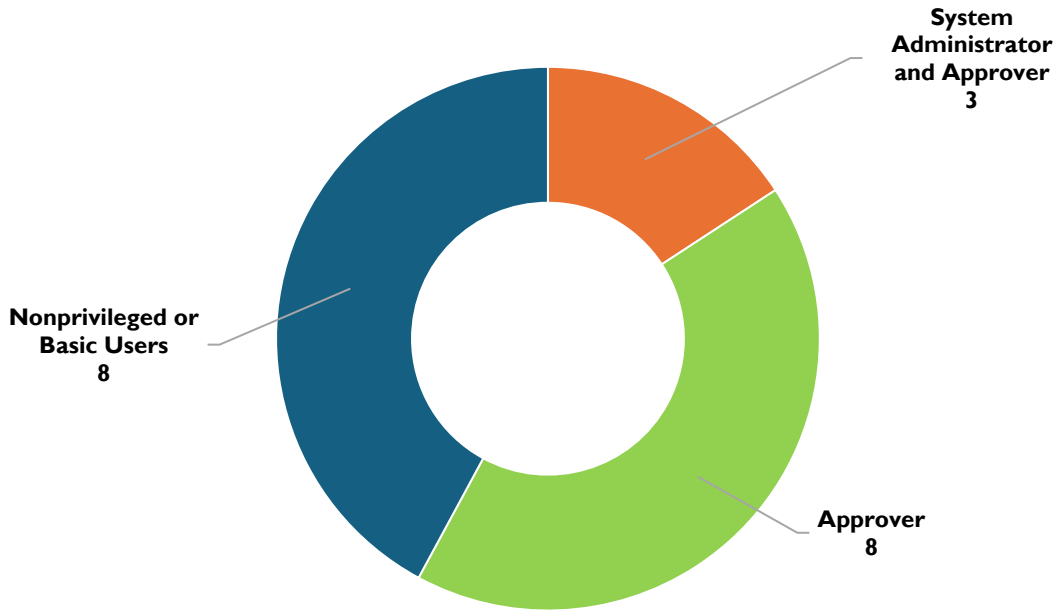
Figure 3. E2 User Account Access After Separation Date as of January 13, 2025



Source: OIG-generated graph from E2 and staffing pattern data from December 2023 through November 2024, as of January 13, 2025.

Of the separated users that continued to log-in to E2, we found that 57 percent (11 of 19) had an elevated system access level (see Figure 4). Specifically, 15 percent of users (3 of 19) had system administrator access—allowing them to perform sensitive tasks, such as creating and disabling users and changing approvers—and could approve travel authorizations and vouchers. The remaining 42 percent of users (8 of 19) had access that allowed them to approve travel authorizations and vouchers.

Figure 4. Access Level of Separated Users Who Continued to Log-in to E2, as of January 13, 2025



Source: OIG-generated graph from E2 and staffing pattern data from December 2023 through November 2024, as of January 13, 2025.

USAID did not disable these accounts, as required, for three main reasons. First, according to Agency officials, TTD had a contract for an Information System Security Officer to perform system security, reporting, higher-level information technology functions, and system reviews.[10] However, the contract ended, leaving TTD without anyone with knowledge to perform those functions. Second, the system owner and other TTD officials stated they were not informed about or aware of Agency policies for disabling E2 accounts. Third, ADS 545 contains inconsistencies that make it unclear when to disable accounts. Section 545.3.14.4 explains that system access must be disabled within 24 hours after an individual's employment ends.[11] In contrast, section 545.3.2.2 requires the Agency to establish a process for notifying account managers within 3 days of an employee's separation,[12] and the system security plan for E2 aligns with this policy.[13] This discrepancy creates a gap where access to the system may not be

[10] ADS 545.2, *Primary Responsibilities*, states that an Information System Security Officer should ensure appropriate security controls are maintained and serve as the primary contact for a system's security matters.
[11] ADS 545.3.14.4, *Personnel Termination (PS-4)*.
[12] ADS 545.3.2.2, *Account Management (AC-2)*.
[13] According to NIST, Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, September 2020, a "system security plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems."

revoked in a timely manner, potentially giving terminated employees continued access to sensitive information. Furthermore, although USAID automatically disables E2 accounts after 90 days of inactivity, separated users can stop their accounts from being disabled automatically by continuing to log in.

Failing to disable unneeded E2 user accounts in a timely manner exposes sensitive USAID information, such as travel, personally identifiable, and credit card information. This creates a risk to millions of dollars processed through the system each year. For example, unauthorized users could:[14]

- Change travel plans, causing delays or cancellations that hinder the employees' ability to provide oversight of critical developmental and humanitarian assistance projects.
- Access and disclose sensitive travel plans, which may ultimately endanger the lives of employees who frequently travel to high-risk or conflict-prone countries.
- Access credit card or personally identifiable information ultimately leading to costly fraudulent transactions, liability for monetary losses, and loss of trust with Agency employees and the public.
- Potentially, in collusion with financial management staff, create fictitious travel transactions for the purchase of plane tickets, rental cars, and hotels.

Given the ongoing transition and evolving future of USAID and foreign assistance, it is critical that the Agency, or its successor, strengthen controls around sensitive travel data. These vulnerabilities put Agency systems at risk of fraud and misuse by rogue actors and warrant the immediate attention of Agency officials.

Therefore, we recommend that USAID's Chief of Travel and Transportation:

Recommendation 1. Review the list of 33 separated users whose accounts in the End-to-End Travel system that have no record of being disabled and, if they are not needed, disable them.

Recommendation 2. Determine the activities of 11 separated users who logged into the End-to-End Travel system after their termination dates and take appropriate action.

Recommendation 3. Designate an Information System Security Officer to perform security functions for the End-to-End Travel system in accordance with USAID policy.

[14] A user may have elevated privileges in E2 allowing them to, for example, add users, modify workflows, or view other individuals' information.

Recommendation 4. Revise the system security plan to require account managers for the End-to-End Travel system to be notified about personnel separations in a timely manner and receive sufficient time to disable system access within 24 hours, rather than 3 days, of a user's separation.

In addition, we recommend that the Chief Information Officer:

Recommendation 5. Revise Agency information systems security policies to eliminate conflicting language for the timeframe to disable accounts for separated employees.

We provided our draft management advisory to USAID on April 10, 2025, and received the Agency's response, which is included as Appendix B, on April 29, 2025.

After reviewing USAID's response to the draft report and subsequent correspondence, we acknowledge management decisions for Recommendations 1, 2, and 5. We consider Recommendations 1 and 2 to be resolved but open pending completion of planned activities. We closed Recommendation 5 because according to USAID, the Agency's policies no longer exist and therefore cannot be revised.

For Recommendation 3, USAID agreed with the intent but explained that the Agency has limited resources due to the transfer of critical business operations to the Department of State (State). Therefore, it cannot assign an Information System Security Officer to the travel system. Also, in its comments, USAID said E2 will be eliminated. However, E2 is on a recent list of systems that USAID plans to transfer to State, which Agency officials confirmed while we were finalizing this memorandum. Considering the risk to sensitive travel data, the pervasiveness of weaknesses identified in this evaluation, and that the Agency plans to transfer E2 to State, it is critical that someone perform these functions. Accordingly, we disagree with this management decision and strongly urge USAID to develop a plan of action, unless the Agency ultimately decommissions E2.

For Recommendation 4, USAID agreed but explained that the Agency cannot meet the timeframes to disable accounts due to limited resources. Considering the concerns discussed above, it is imperative that USAID disable accounts in a timely manner, unless the Agency's Chief Information Officer allows a deviation from this requirement. Therefore, we disagree with this management decision and strongly urge USAID to develop a plan to disable these accounts, unless the Agency ultimately decommissions E2.

We appreciate the assistance you and your staff provided to us during this evaluation.

Appendix A. Scope and Methodology

We conducted this evaluation from December 3, 2024, to April 10, 2025, in accordance with Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspections and Evaluations*.

Our objective was to assess the extent to which USAID disabled user accounts for E2 in accordance with Agency policy.

We focused on E2 data from December 1, 2023, through November 30, 2024, and focused on accounts for employees who separated from the Agency.[15] We conducted our work in Washington, DC.

To answer our objective, we reviewed E2 data from December 1, 2023, through November 30, 2024, focusing primarily on account status (enabled or disabled), disabled dates, and last login dates. We also reviewed two USAID staffing reports, which listed Agency employees as of December 16, 2024, and December 23, 2024. To identify E2 accounts for employees who separated from the Agency during the period of our review, we compared E2 data to the two staffing reports and identified accounts for 178 separate employees. Next, we analyzed the E2 testing universe to determine when USAID disabled accounts for these users as of January 13, 2025. We also analyzed the testing universe to identify users who accessed E2 after separation. We interviewed E2 Helpdesk officials regarding the reliability of the data. Based on the interview, we determined that the data was sufficiently reliable for the purpose of our objective.

In addition, we reviewed ADS 545 to identify requirements for disabling user access to USAID systems and interviewed officials from TTD to understand how the Agency implements these requirements for E2.

[15] We did not evaluate accounts disabled due to inactivity.

Appendix B. Agency Comments

MEMORANDUM

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

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

DATE: April 17, 2025

SUBJECT: Management Comments to Respond to the Office of Inspector General's (OIG) Draft Management Advisory titled, *Information Security: Weaknesses in USAID's Management of Travel System Account Closures Highlight Concerns About Protecting Travelers and Sensitive Information* (Report No. A-000-25-002-M)

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, and has no comments regarding the content of the report.

USAID has significantly downsized and will continue to do so with the end state to transition critical business operations to the Department of State (DoS). This involves eliminating the majority of USAID's applications and systems as part of the Agency's drawdown effort, including USAID's End-to-End Travel system known as E2. At this time and for the foreseeable future, E2 is minimally maintained for the purpose of offboarding USAID staff that are departing the Agency. Additionally, USAID has resource constraints both Direct Hire and limited contractor support due to a high number of contract terminations over the past three months. That includes Chief of Travel and Transportation, Jamie Bishop, who has retired. Please keep in mind this context for our management comments.

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, *INFORMATION SECURITY: WEAKNESSES IN USAID'S MANAGEMENT OF TRAVEL SYSTEM ACCOUNT CLOSURES HIGHLIGHT CONCERNS ABOUT PROTECTING TRAVELERS AND SENSITIVE INFORMATION* (Report No. A-000-25-002-M)

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 five recommendation(s) for USAID:

Recommendation 1. Review the list of 33 separated users whose accounts in the End-to-End Travel system that have no record of being disabled and, if they are not needed, disable them.

- **Management Comments:** USAID agrees with this recommendation. USAID requests OIG provide the list of 33 separated user accounts identified so that we may review and disable them.

Recommendation 2. Determine the activities of 11 separated users who logged into the End-to-End Travel system after their termination dates and take appropriate action.

- **Management Comment:** USAID agrees with this recommendation. USAID requests OIG provide the list of 11 separated user accounts so that we may review and take appropriate action.

Recommendation 3. Designate an Information System Security Officer to perform security functions for the End-to-End Travel system in accordance with USAID policy. A user may have elevated privileges in E2 allowing them to, for example, add users, modify workflows, or view other individuals' information.

- **Management Comment:** USAID agrees with the intent of this recommendation. USAID will continue to provide operation and maintenance support for E2, along with continuous monitoring of the system to the best of our ability to minimize risks. However, USAID has limited ability to provide an ISSO for this system due to limited resources and contract terminations.

Recommendation 4. Revise the system security plan to require account managers for the End-to-End Travel system to be notified about personnel separations in a timely manner and receive sufficient time to disable system access within 24 hours, rather than 3 days, of a user's separation.

- **Management Comment:** USAID agrees with this recommendation. USAID has limited ability to revise the system security plan for E2 and meet the deadlines noted due to limited resources and contract terminations.

Recommendation 5. Revise Agency information systems security policies to eliminate conflicting language for the timeframe to disable accounts for separated employees.

- **Management Comment:** USAID agrees with this recommendation. However, USAID's Automated Directives System (ADS), Chapter 545, Information Systems Security, which defines the security policies for all information systems owned by or operated on behalf of USAID, no longer exists. Therefore, we are unable to revise the language as requested.

In view of the above, we request that the OIG inform USAID when it agrees or disagrees with a management comment.