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

FISMA: Overall Effectiveness of USAID's Information Security Program for FY 2026 Could Not Be Determined

Report A-000-27-001-M
November 23, 2026

Evaluation



Office of Audits, Inspections, and Evaluations

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

DATE: November 23, 2026

TO: Bill Woolf
Performing the Duties of Administrator
U.S. Agency for International Development

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

SUBJECT: FISMA: Overall Effectiveness of USAID's Information Security Program for FY 2026 Could Not Be Determined

This memorandum transmits the final evaluation of USAID's information security program for fiscal year 2026 in support of the Federal Information Security Modernization Act of 2014 (FISMA). Our objective was to determine whether USAID implemented an effective information security program.

USAID did not provide formal management comments on the draft report. Instead, the Agency provided technical comments, which we incorporated as appropriate. Should we receive formal comments from the Agency on this report at a later date, we will update and reissue the report to reflect those comments as applicable.

The report contains two new recommendations related to USAID's information security program and identifies nine recommendations from prior FISMA assessments that USAID has not yet addressed. We consider all 11 recommendations open and unresolved. Please provide us with a management decision for each of the two new recommendations, including agreement or disagreement with the recommendation and a plan and target date for corrective action. Please provide evidence of final action to OIGAuditTracking@usaid.gov.

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

Contents

Report in Brief 1
Introduction 2
Background 3
FISMA Requirements 3
Transition of USAID's IT Applications and System Infrastructure to the Department of State 3
Prior OIG FISMA Oversight Work 4
USAID's Delayed Responses Prevented OIG From Fully Assessing the Agency's FY 2026 Information Security Program, and OIG's Prior Recommendations Were Unaddressed 4
USAID Generally Had Policies and Procedures for Its Information Security Program, but Delayed Responses Prevented OIG From Assessing Whether the Agency Implemented Key Controls 4
USAID Has Not Addressed Five Prior Recommendations to Strengthen Its Information Security Program 6
Conclusion 7
Recommendations 7
OIG Response to Agency Comments 7
Appendix A. Scope and Methodology 8
Appendix B. Prior Open Recommendations 9

Report No A-000-27-001-M
November 23, 2026

Report in Brief

Why We Did This Evaluation

Implementing an effective information security program is crucial for protecting the confidentiality, integrity, and availability of Federal agencies' systems and the information they contain. Such safeguards address threats, ultimately protecting Americans and government resources from bad actors. To that end, the Federal Information Security Modernization Act of 2014 (FISMA) directs OIG to annually assess the effectiveness of the U.S. Agency for International Development's (USAID) information security program and practices and report the results of the assessments to the Office of Management and Budget (OMB).

On March 28, 2025, the Secretary of State announced that USAID would cease operating as an independent agency. On July 1, 2025, the Department of State (State) assumed responsibility for many of the Agency's functions and its ongoing programming. Remaining USAID personnel were responsible for managing the closeout of terminated awards and the transition of the Agency's independent operations. While State has provided limited IT services during this transition, USAID continues to be responsible for certain IT functions and its information security program until the wind-down is complete.

In accordance with FISMA, we conducted this evaluation to determine whether USAID had implemented an effective information security program for fiscal year (FY) 2026 through July 21, 2026, the date we submitted the results of our assessment to OMB.

What We Recommend

We made two new recommendations for USAID to provide information regarding its information security program and address identified weaknesses. We also referenced nine prior recommendations that the Agency has not addressed. In total, 11 recommendations are open and unresolved.

What We Found

USAID generally had policies and procedures for its information security program, but delayed responses prevented OIG from assessing whether the Agency implemented key controls. We determined that USAID generally had policies and procedures in place for its information security program as OMB and CIGIE required. However, we could not determine the overall effectiveness of USAID's information security program in FY 2026 because the Agency did not provide us with sufficient, appropriate evidence in a timely manner to allow us to conduct our assessment by OMB's July 31, 2026, deadline. USAID did not begin to provide documents to us until more than 2 months after we announced our evaluation, and some documents submitted were outdated. Agency officials said they were focused on the transition to State and questioned our authority to conduct the evaluation.

USAID has not addressed nine prior recommendations to strengthen its information security program. The recommendations we made in the FY 2025 evaluation pertain to conducting risk and security control assessments, including cybersecurity duties in position descriptions and performance plans, and implementing mechanisms to handle noncompliant devices on the network. USAID has also not addressed four recommendations from our FY 2020 and 2024 FISMA audits focused on disabling network accounts and maintaining certain records of staff members.

Even though USAID is in the process of winding down its operations, the Agency still has a responsibility to ensure it has an effective information security program, which includes addressing our open recommendations to improve that program.

Introduction

Implementing an effective information security program is crucial for protecting the confidentiality, integrity, and availability of Federal agencies' systems and the information they contain. Such safeguards address threats, ultimately protecting Americans and government resources from bad actors. To that end, the Federal Information Security Modernization Act of 2014 (FISMA)[1] directs OIG to annually assess the effectiveness of USAID's information security program and practices and report the results of the assessments to the Office of Management and Budget (OMB).[2]

On March 28, 2025, the Secretary of State announced that USAID would cease operating as an independent agency. On July 1, 2025, the Department of State (State) assumed responsibility for many of the Agency's functions and its ongoing programming. Remaining USAID personnel were responsible for managing the closeout of terminated awards and the wind-down of the Agency's independent operations. While State has provided limited IT services during this transition, USAID continues to be responsible for certain IT functions and its information security program until the wind-down is complete.

In accordance with FISMA, we conducted this evaluation to determine whether USAID had implemented an effective information security program.[3] Our review focused on USAID's information security program for fiscal year (FY) 2026 through July 21, 2026, the date we submitted the results of our assessment to OMB.

To assess the effectiveness of USAID's information security program, we followed OMB and the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) IG FISMA reporting metrics and the Inspector General FISMA evaluator's guide.[4] Ultimately, we were unable to complete the procedures needed to answer our evaluation objective for reasons we discuss later in the report. Despite this limitation, we reviewed regulatory requirements and analyzed the Agency's policies and procedures for its information security program in areas including: (1) supply chain, (2) configuration management, (3) identity and access control, (4) security awareness training, and (5) continuous monitoring controls. We compared these policies and procedures against requirements stipulated in the FISMA evaluator's guide. We obtained from USAID officials in the Office of the Chief Information Officer (OCIO) testimonial information about the systems in the Agency's inventory, State's role in securing USAID systems, the status of USAID's policies and procedures, and the effect of reduced staffing on the Agency's ability to implement key controls.

[1] Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551-3558).
[2] 44 U.S.C. § 3555, Annual Independent Evaluation.
[3] For this evaluation, an effective information security program is defined as having an overall mature program based on the FY 2025 IG FISMA reporting metrics.
[4] On March 17, 2026, OMB and CIGIE instructed OIGs in FY 2026 to follow *FY 2025 Inspector General - Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, April 3, 2025, and *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide*, Version 1.0, May 5, 2025.

We conducted our work from March to September 2026 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Appendix A provides more detail on our scope and methodology.

Background

FISMA Requirements

FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other sources. The statute requires agency heads to implement policies and procedures to protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

OMB and CIGIE provide instructions on assessing agency information security programs to IGs.[5] To help facilitate these assessments, the instructions contain a set of metrics that IGs must evaluate. IGs were to submit the results of these assessments to OMB by July 31, 2026.

Various requirements are in place to help USAID implement an effective information security program. For example, the National Institute of Standards and Technology (NIST) issued a catalog of security and privacy controls, which includes the need to perform security control assessments and track weaknesses.[6]

Transition of USAID's IT Applications and System Infrastructure to the Department of State

The transition of USAID functions and programs to State in 2025 resulted in significant changes to the Agency's operations and staffing. Most Agency staff were terminated, including from OCIO. The OCIO is responsible for overseeing the security posture of information systems and implementing policies to protect the Agency's systems from bad actors. The Deputy Chief Information Officer in OCIO was responsible for certain IT security functions.

On February 3, 2026, USAID and State signed a memorandum of agreement that outlined the IT services State would perform for USAID. According to the agreement, State's services were limited to supporting the applications and system infrastructure needed for USAID to draw down and conduct other supporting activities. USAID maintained responsibility for working with State to ensure that system access, device management, and user support complied with IT security requirements.

[5] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, April 3, 2025.
[6] NIST, Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

Prior OIG FISMA Oversight Work

In our FY 2025 FISMA evaluation, we concluded that USAID implemented an effective information security program as of April 14, 2025.[7] However, we identified weaknesses and made five recommendations to address them. We determined that USAID had not yet addressed four recommendations we made in our FY 2020 and FY 2024 reports.

USAID's Delayed Responses Prevented OIG From Fully Assessing the Agency's FY 2026 Information Security Program, and OIG's Prior Recommendations Were Unaddressed

Although USAID generally had policies and procedures for its information security program, delayed responses prevented us from assessing whether the Agency implemented key controls. We also found that USAID had not taken actions to address nine recommendations we made in prior years to strengthen the Agency's information security program.

USAID Generally Had Policies and Procedures for Its Information Security Program, but Delayed Responses Prevented OIG From Assessing Whether the Agency Implemented Key Controls

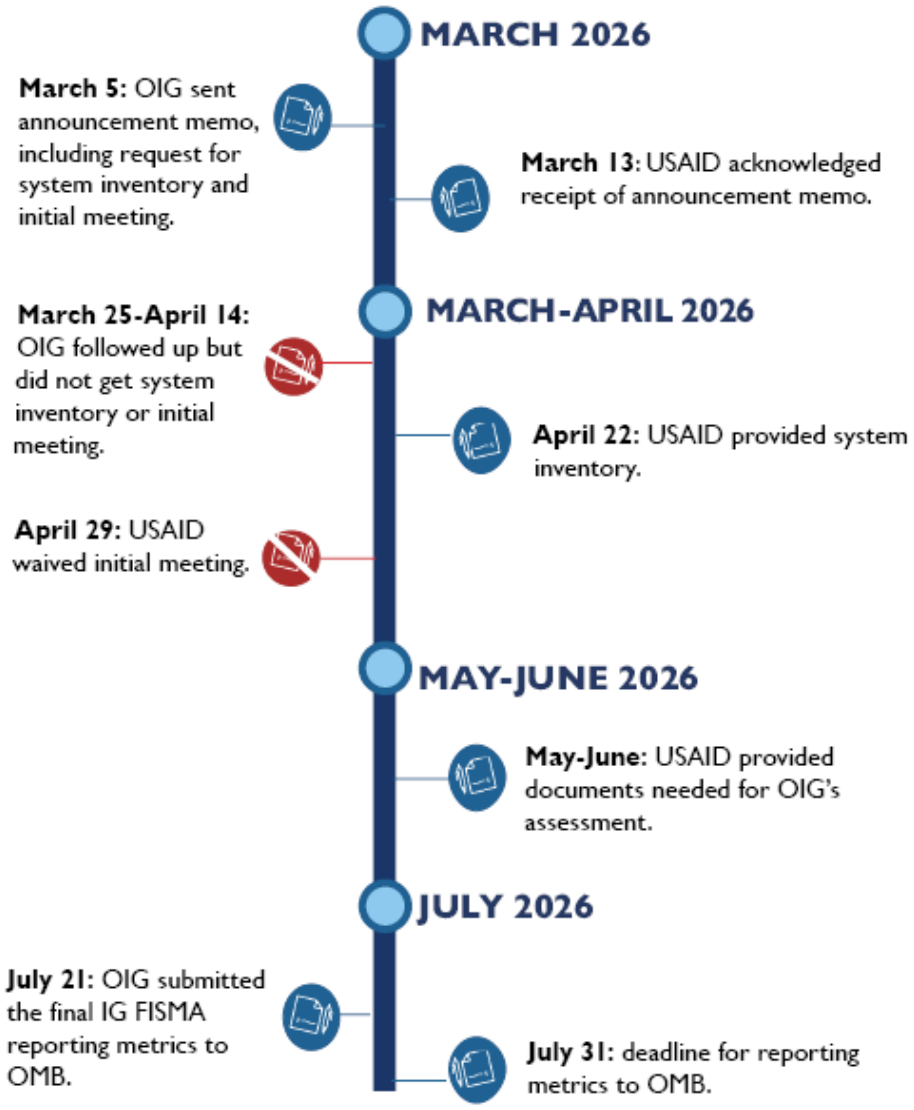
We determined that USAID generally had policies and procedures in place for its information security program as OMB and CIGIE required. For example, we verified that USAID had policies and procedures for (1) supply chain, (2) configuration management, (3) identity and access control, (4) security awareness training, and (5) continuous monitoring controls.

However, we could not determine the overall effectiveness of USAID's information security program in FY 2026 because the Agency did not provide us with sufficient, appropriate evidence in a timely manner to allow us to conduct our assessment by OMB's July 31, 2026, deadline. For example, USAID did not provide evidence that it had developed policies and procedures for its data inventories. We also did not receive the information needed to assess whether the Agency terminated unneeded access to its systems in a timely manner—a key control given that staff are separating from the Agency as it winds down.

USAID did not begin to provide documents to us until May 2026, more than 2 months after we announced our evaluation, and some of the documents were outdated. For example, Agency officials provided us with a 2021 version of the information security policy, while we had access to a 2025 version from our prior FISMA evaluation. Figure 1 shows key events between our March 2026 announcement of the evaluation and submission of FISMA metrics to OMB.

[7] USAID OIG, *FISMA: USAID Implemented an Effective Information Security Program Through April 14, 2025, Despite Some Concerns* (A-000-26-004-M), March 4, 2026.

Figure 1. Key Events Affecting OIG's Fiscal Year 2026 FISMA Evaluation



Source: OIG's summary of significant events during the FISMA evaluation.

According to USAID officials, we did not take the Agency's operational status into account, given that it began shutting down operations in 2025 and continued to do so in 2026. Further, because USAID was transferring its IT systems to State, the officials questioned whether USAID OIG or State OIG should evaluate the Agency's information security program. According to a USAID official responsible for information security, as part of this transition, State assumed responsibility for implementing and operating the majority of applicable FISMA and NIST security controls. According to this official, USAID also no longer owned or operated its IT infrastructure or other core IT capabilities.

As long as USAID exists, however, we are responsible for oversight of its programs and operations. FISMA requires the Agency to have an information security program and USAID

OIG to annually assess its effectiveness. Moreover, the Agency is required to follow NIST requirements to assess and report on the security controls of its information systems.[8] USAID must also develop a plan of action and milestones to correct weaknesses noted during the assessment of the controls in accordance with NIST requirements.[9]

Even as USAID transfers its information systems to State, the Agency is responsible for the effectiveness of its information security program. Otherwise, USAID does not have assurance that it has implemented all the controls necessary to protect its information. Moreover, not providing timely information about its information security program and controls prevents us from conducting required oversight of this critical Agency program. Accordingly, we cannot assure Congress and American taxpayers that USAID has adequate safeguards to protect government IT resources and systems. Such safeguards would mitigate significant risks, including unauthorized access to systems and disclosure or manipulation of sensitive information.

USAID Has Not Addressed Nine Prior Recommendations to Strengthen Its Information Security Program

USAID has not addressed five recommendations to correct weaknesses that we identified in our FY 2025 FISMA evaluation and four recommendations we made in prior years. The recommendations we made in the FY 2025 evaluation pertain to conducting risk and security control assessments, including cybersecurity duties in position descriptions and performance plans, and implementing mechanisms to handle noncompliant devices on the network. USAID did not submit information to us indicating that it took corrective actions in those areas. We also recommended that the Agency document policies and procedures for data inventories, but USAID did not provide evidence that it took any action this year.

In addition, USAID has not addressed four previous recommendations from our FY 2020 and FY 2024 FISMA audits focused on disabling network accounts and maintaining certain records of staff members.

Even though USAID is in the process of transitioning its operations to State, it still has a responsibility to ensure it has an effective information security program, which includes addressing our open recommendations to improve that program. Appendix B provides more detail on those recommendations.

[8] NIST, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* CA-2 (d) and (e), "Control Assessment," September 2020.
[9] NIST, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* CA-5 (a), "Plan of Action and Milestones," September 2020.

Conclusion

Having an effective information security program is essential for protecting USAID's information systems and the information they contain, particularly given significant changes in the Agency's operations over the past year. Because USAID did not provide us with timely evidence to assess the effectiveness of its information security program, as FISMA requires, we could not conduct a full evaluation of the program by OMB's deadline. Thus, Congress and American taxpayers do not have reasonable assurance that USAID has adequate safeguards to protect government resources. Lack of insight into the Agency's information security program and implementation of key controls—along with its failure to address prior weaknesses—increase the risk to systems that hold critical information. Taking immediate corrective actions to address these weaknesses and strengthen its information security program is crucial for USAID to ensure it has effective controls to protect the confidentiality, integrity, and availability of its resources from bad actors.

Recommendations

We recommend that USAID's Office of the Chief Information Officer take the following actions:

1. Provide information that demonstrates whether USAID has an effective information security program, including a written security controls assessment of the Agency's information systems and operational environment.
2. Develop and implement a corrective action plan, including milestones and target dates, to address any weaknesses USAID identified in the security controls assessment as well as weaknesses OIG has previously identified in the Agency's information security program.

OIG Response to Agency Comments

We provided our draft report to USAID on September 22, 2026. As of November 23, 2026, the Agency had not provided formal management comments on the draft report. Instead, the Agency provided technical comments, which we incorporated as appropriate. Should the Agency provide formal comments at a later date, we will update and reissue the report to reflect those comments as applicable. We consider the two recommendations open and unresolved.

Appendix A. Scope and Methodology

We conducted our work from Washington, DC, from March to September 2026 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Our objective for this evaluation was to determine whether USAID implemented an effective information security program. Our review focused on USAID's information security program for FY 2026 through July 21, 2026, the date we submitted the final IG FISMA reporting metrics to OMB.

To answer our objective, we followed the IG FISMA reporting metrics and IG FISMA evaluator's guide, which provides a baseline of suggested evidence and test steps for FISMA-related assessments. Ultimately, we were unable to complete the procedures needed to answer our objective. As discussed in the report, USAID did not provide us with sufficient, appropriate evidence in a timely manner before OMB's July 31, 2026, deadline.

Despite not receiving timely information from USAID, we were able to test certain aspects of the metrics identified in OMB and CIGIE's IG FISMA reporting metrics.[10] Specifically, we reviewed USAID's policies, procedures, plans, and strategies to determine whether the Agency documented key aspects of its information security program. For example, we compared USAID's policies and procedures for (1) supply chain, (2) configuration management, (3) identity and access control, (4) security awareness training, and (5) continuous monitoring controls to the IG FISMA evaluator's guide.[11] We also obtained testimonial evidence from USAID officials in the Office of the Chief Information Officer responsible for the information security program. The officials discussed the systems in the Agency's inventory, State's role in securing USAID systems, the status of USAID's policies and procedures, and the effect of reduced staffing on the Agency's ability to implement key controls.

We determined the status of recommendations we made to USAID in our FY 2020, FY 2024, and FY 2025 FISMA reports, which were open at the beginning of evaluation fieldwork. Specifically, we assessed OIG records to determine whether the Agency provided evidence that it took corrective actions to implement those recommendations.[12]

[10] OMB and CIGIE, *FY 2025 Inspector General - Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, April 3, 2025.
[11] OMB and CIGIE, *FY 2025 IG FISMA Metrics Evaluator's Guide*, Version 1.0, May 5, 2025. USAID, Automated Directives System, Chapter 545, Information System Security, January 16, 2025.
[12] USAID OIG, *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (A-000-21-004-C), January 7, 2021; *FISMA: USAID Implemented an Effective Information Security Program for Fiscal Year 2024 but Longstanding Weaknesses Persist* (A-000-24-005-C), September 19, 2024; and *FISMA: USAID Implemented an Effective Information Security Program Through April 14, 2025, Despite Some Concerns* (A-000-26-004-M), March 4, 2026.

Appendix B. Prior Open Recommendations

The following table provides the recommendations from our FY 2020, FY 2024, and FY 2025 FISMA reports that were open as of October 1, 2025, the beginning of the evaluation period.[13]

Table 1. Prior Open Recommendations

Report & Recommendation #	Recommendation	USAID's Position	OIG's Position
A-000-26-004-M (FY 2025, Rec. 1)	We recommend that USAID's Office of the Chief Information Officer conduct updated risk assessments for the two systems we identified.	Open	Open
A-000-26-004-M (FY 2025, Rec. 2)	We recommend that USAID's Office of the Chief Information Officer perform security controls assessments for the two systems we identified.	Open	Open
A-000-26-004-M (FY 2025, Rec. 3)	We recommend that USAID's Office of the Chief Information Officer determine whether the Agency included cybersecurity duties in position descriptions and performance plans. If not, take corrective action, including addressing the causes for not doing so.	Open	Open
A-000-26-004-M (FY 2025, Rec. 4)	We recommend that USAID's Office of the Chief Information Officer determine whether the Agency developed and implemented policies and procedures for maintaining data and metadata inventories for its various data types, including data from third-party providers. If not, take corrective action, including addressing the causes for not doing so.	Open	Open
A-000-26-004-M (FY 2025, Rec. 5)	We recommend that USAID's Office of the Chief Information Officer determine whether the Agency implemented network monitoring and enforcement mechanisms to identify and disconnect or isolate noncompliant devices. If not, take corrective action, including addressing the causes for not doing so.	Open	Open
A-000-24-005-C (FY 2024, Rec. 1)	We recommend that USAID's Chief Information Officer request its cognizant Management Council on Risk and Internal Control to report and track as a significant deficiency to the Agency the risk of not timely disabling network accounts for separated employees and contractors, as identified in Office of Inspector General Report No. A-000-21-004-C, Recommendation 2.	Open	Open

[13] USAID OIG, *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (A-000-21-004-C), January 7, 2021; *FISMA: USAID Implemented an Effective Information Security Program for Fiscal Year 2024 but Longstanding Weaknesses Persist* (A-000-24-005-C), September 19, 2024; and *FISMA: USAID Implemented an Effective Information Security Program Through April 14, 2025, Despite Some Concerns* (A-000-26-004-M), March 4, 2026.

Report & Recommendation #	Recommendation	USAID's Position	OIG's Position
A-000-24-005-C (FY 2024, Rec. 2)	We recommend that USAID's Chief Human Capital Officer request its cognizant Management Council on Risk and Internal Control to report and track as a significant deficiency to the Agency the risk of not maintaining records evidencing that staff have been off-boarded in accordance with Agency policy, as identified in Office of Inspector General Report No. A-000-21-004-C, Recommendation 3.	Open	Open
A-000-21-004-C (FY 2020, Rec. 2)	We recommend that USAID's Chief Information Officer should collaborate with the Office of Human Capital and Talent Management to document and implement a process to verify that separated employees' accounts are disabled in a timely manner in accordance with USAID policy.	Open	Open
A-000-21-004-C (FY 2020. Rec. 3)	We recommend that USAID's Chief Human Capital Officer should implement a process to maintain records electronically for onboarding and offboarding staff.	Open	Open

Source: OIG's FY 2020, FY 2024, and FY 2025 FISMA assessment reports and OIG records.

Visit our website at oig.usaid.gov and
follow us on social media.

X: @AidOversight
LinkedIn: USAID Office of Inspector General
Instagram: @usaid.oig



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

Report Waste, Fraud, and Abuse
Online Complaint Form