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

MANAGEMENT ADVISORY

DATE: May 29, 2026

TO: Elisabeth Feleke
Chief Program Officer
U.S. African Development Foundation

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

SUBJECT: U.S. African Development Foundation's Lack of Responsiveness to Oversight Matters Limits Transparency Into Agency Operations and Management of Funds (Report No. A-ADF-26-005-A)

We are writing to alert you about an ongoing lack of information and insight into the U.S. African Development Foundation's (USADF) operations and management of funds. Congress has charged the USAID Office of Inspector General (OIG) with overseeing the entirety of USADF's funding and operations, but the continued lack of response from Agency officials jeopardizes OIG's ability to carry out that mandate. This includes OIG conducting mandatory assessments of: the Agency's information security program and practices; financial management assessments; and discretionary reviews of other areas, including the status of millions of dollars' worth of physical and monetary assets overseas.

Without providing OIG with this information, Congress and American taxpayers lack reasonable assurance that USADF has adequate safeguards to protect government resources. Such safeguards would mitigate significant operational and financial risks, including unauthorized access to systems, disclosure or manipulation of sensitive information, misuse of funds and assets, and unreported instances of fraud. These risks could result in financial losses, legal exposure, and lasting reputational harm to the U.S. government.

As long as USADF remains operational, it is imperative that the Agency actively manages risks to its information security program, financial management, and strategic partnerships and grants. USADF must maintain an effective information security program to safeguard sensitive information and produce accurate and reliable financial statements to ensure accountability and transparency. Additionally, USADF must address longstanding weaknesses in its strategic partnership and grant management processes to safeguard taxpayer dollars and other donor funding.

We strongly urge USADF officials to keep OIG updated about the status of its efforts to restore access to its systems and records and respond to our information requests. Doing so will enable us to provide timely, relevant, and impactful oversight that can inform USADF,

Congress, and other stakeholders about the Agency's operations, the potential risks to those operations, and steps the Agency can take to address those risks.

Summary

As of this writing, USADF continues to be nonresponsive to our information requests for two statutorily mandated assessments critical to ensuring controls over information technology systems and safeguarding taxpayer funds. The required fiscal year (FY) 2026 assessment of USADF's information security program and the audit of its financial statements are due July 31, 2026, and November 16, 2026, respectively. Between March/April 2025 and January 2026, USADF leadership did not provide the information we needed to complete these assessments for FY 2025. In addition, USADF has not addressed 11 of our 12 open recommendations, some dating back as far as August 2024, related to addressing fraud risks in the Agency's grants management activities.

According to a senior USADF career official, nearly all staff were placed on administrative leave or terminated in 2025, then reinstated, and later placed back on administrative leave. As a result, USADF could not provide the documentation we needed to complete our evaluation of its information security program in FY 2025. One senior official told us that USADF staff did not have access to systems at various periods of time, and another official said that staff have been attempting to regain full system access since March 17, 2026.[1] Agency officials told us that they are waiting for responses from the Department of the Treasury and Office of Management and Budget (OMB) regarding their access to systems and records. They have also asked USADF's information management service provider to restore access to official emails and electronic files but have yet to receive a response.

If USADF does not respond to our information requests, we cannot complete our mandatory assessments and other planned oversight, including the verification of USADF's physical assets and over $9 million in accounts overseas.[2]

Furthermore, decision makers will lack the reliable information on USADF's operations and programming they need to allocate resources effectively and responsibly and to address risks to information security, financial, and strategic partnerships and grants management. Vulnerabilities may go undetected due to a lack of insight into the security of USADF's information systems and financial management practices. Such vulnerabilities create opportunities for fraudsters and other unauthorized actors to exploit weaknesses or gain access to protected data. Also, as we have reported before, persistent gaps in strategic partnership and grants management further increase the likelihood that instances of fraud will go unreported and Federal funds will be misused.

[1] Pursuant to a recent court decision, USADF staff have returned to duty. See *Rural Development Innovations Ltd, et al v. Marocco*, et al, No. 25-1631 (D.D.C. April 27, 2026).
[2] This amount is included in USADF's unaudited financial statements as of September 30, 2025.

USADF's Lack of Responses Prevented OIG From Assessing Information Security Risks

USADF did not provide information OIG requested from April 14, 2025, through January 13, 2026, for our assessment of its information security program for FY 2025.[3] The Federal Information Security Modernization Act of 2014 (FISMA) requires OIG to complete the assessment annually and submit the results to OMB. Thus, on January 13, we reported that we could not assess the effectiveness of USADF's information security program for protecting the confidentiality, integrity, and availability of its systems and the information they contain.[4]

Specifically, USADF did not:

- Provide evidence that it implemented controls in 8 of 25 areas of its information security program. For example, USADF did not provide evidence that it could detect, analyze, and handle security incidents. As a result, USADF may not have the ability to respond quickly to cyberattacks.
- Provide management decisions, as OMB requires, for the five recommendations to address weaknesses we identified in our January 2026 report[5]: remediating serious vulnerabilities on a USADF information system; defining roles, responsibilities, and authority for managing cybersecurity risks; and updating cybersecurity training plans based on needs of its workforce. The failure to address these weaknesses increases the risk that a bad actor may obtain unauthorized access to USADF's systems and change or disclose sensitive information.
- Take corrective action to address two recommendations from our prior audit of its information security program.[6] One recommendation pertains to conducting reinvestigations of staff who have access to sensitive information, such as information that can be used to gain unauthorized access to USADF's systems. The other focuses on improving information security training for staff who have access to sensitive information. USADF's target dates for final actions on these recommendations were over a year ago: November 30, 2024, and December 30, 2024, respectively. Taking these actions will allow USADF to decrease the risk of loss, misuse, and unauthorized changes to sensitive information on its systems.

In February 2026, we initiated our evaluation of USADF's information security program for FY 2026. On March 6, we made our initial request to USADF for its systems inventory and information security policies and procedures. However, as of May 15, the Agency had not provided the requested information. If we do not receive this key information, we will not be able to complete our assessment. Further, stakeholders will not have insight into USADF's information security program and practices, which could put sensitive information at risk.

---

[3] USADF officials provided feedback on our findings during our December 2025 exit conference.
[4] USAID OIG, *FISMA: Overall Effectiveness of USADF's Information Security Program for FY 2025 Could Not Be Determined and Weaknesses Exist* (A-ADF-26-001-M), January 13, 2026.
[5] OMB, *Transmittal of Revised OMB Circular A-50, Audit, Inspection, or Evaluation Follow-Up* (M-25-01), November 7, 2024.
[6] Recommendations 2 and 7 in USAID OIG, *FISMA: Despite Weaknesses, USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2024* (A-ADF-24-003-C), August 29, 2024.

USADF's Inconsistent Responses Hindered OIG's Audit of the Agency's FY 2025 Financial Statements

In January 2026, we reported that we could not provide a basis for an audit opinion on USADF's FY 2025 financial statements because the Agency did not consistently respond to our requests for information from March 8, 2025, through January 16, 2026.[7] This lack of response is unprecedented.

Specifically, USADF did not provide:

- A certification about the accuracy of its financial statements and accompanying information or consistent access to its staff during the audit period. This limits the assurance that the public and other stakeholders can have about USADF's overall financial position, internal controls, and compliance with laws and regulations.
- Evidence, such as invoices for grant expenses and purchase of USADF assets, needed to test financial activities, which limits USADF's ability to demonstrate that transactions were legitimate and that it implemented controls to prevent and detect the risk of fraud.
- Responses to our FY 2025 financial statements audit report, including management decisions on the 13 new recommendations, as OMB requires.[8] Moreover, USADF's management did not confirm receipt of the report as it has done previously. Thus, we do not know whether USADF is taking action to address the risks to the Agency's financial statements that we identified.

We have made efforts to start our FY 2026 audit of USADF's financial statements. However, it is unclear whether we will receive responses to our information requests in a timely manner because, according to Agency officials, they do not have access to their own financial management systems. This results in a continued lack of insight into USADF's management of taxpayer funds.

USADF Has Not Addressed Fraud Risks and Weaknesses in Its Strategic Partnerships and Grants That OIG Previously Identified

We previously identified fraud risks and weaknesses in USADF's management of strategic partnerships and grants, but USADF has not demonstrated that it has addressed our 11 open recommendations.[9] For example, in August 2024, we reported that USADF did not report

[7] USAID OIG, *Audit of USADF's Financial Statements for Fiscal Year 2025*(0-ADF-26-003-C), January 16, 2026. In following the Government Management Reform Act of 1994, OMB requires our office to annually express an opinion on whether USADF's financial statements are presented fairly, in all material respects and to evaluate the Agency's internal controls over financial reporting, among other things. OMB Bulletin No. 24-02, *Audit Requirements for Federal Financial Statements*, July 29, 2024.
[8] OMB Circular A-50, *Audit, Inspection, or Evaluation Follow-Up* (M-25-01), November 7, 2024.
[9] The Joint Explanatory Statement for the FY 2026 National Security, Department of State, and Related Programs Appropriations Act requires USADF to respond to OIG and U.S. Government Accountability Office recommendations within 90 days of enactment of the bill on February 3, 2026.

suspected misuse of its grant funding and equipment.[10] Specifically, USADF did not provide evidence that it:

- Developed and implemented a comprehensive risk management framework that included risk assessment procedures, preventive controls, detection mechanisms, response protocols, and regular monitoring and review processes to adjust the framework as necessary. Such a framework helps with the early identification of fraud within USADF's operations. USADF's target date to implement this recommendation was January 31, 2025.
- Provided USADF staff with fraud awareness briefings presented by OIG's Office of Investigations. USADF's target date to implement this recommendation was October 19, 2024. Serious allegations will remain unreported if USADF staff do not know how to promptly identify and report potential fraud, waste, abuse, and mismanagement to OIG.
- Monitored the effectiveness of the fraud risk management framework and the impact of the fraud awareness briefings. USADF set a target date to complete the initial evaluation of the fraud risk management framework and briefings impact on December 31, 2025. This would have allowed USADF to assess the effectiveness of the framework and make adjustments as necessary.

USADF also has not taken action to address gaps we identified in its policies and procedures for its strategic partnership and grants management, despite receiving $12 million in appropriations for FY 2026 to continue its grant activities.[11] In August 2025, we made nine recommendations to strengthen USADF's strategic partnership and grants management and administration processes.[12] USADF agreed with each recommendation and identified planned corrective actions and target dates but stated implementation was contingent on the Agency remaining operational. Taking steps to address these gaps will allow USADF to improve implementation of these taxpayer- and strategic partnership-funded grants.[13] In contrast, unaddressed recommendations mean that USADF risks establishing ineffective strategic partnerships and lacking assurance that its grants management activities will be implemented on time or even at all.

Additionally, uncertainty about staff availability limits USADF's oversight of its overseas operations, including its grant activities and physical and monetary assets. For example, USADF officials told us that they did not know the current balances held in overseas bank accounts—more than $9 million as of September 30, 2025—due to lack of staff with signatory access and ability to travel. We too are concerned about our ability to access records and Agency staff to make timely site visits to inspect physical and monetary assets.

[10] USAID OIG, *Nonreporting of Suspected Misuse of USADF Grant Funds and Equipment* (E- ADF-24-001-A), August 29, 2024.
[11] USADF officials said that they contacted but have not received a response from the Department of State and OMB about releasing appropriated funds for strategic partnership and grant activities.
[12] USAID OIG, *U.S. African Development Foundation: Gaps in Policy and Guidance Hindered Strategic Partnerships and Grants Administration* (E-ADF-25-004-M), August 28, 2025.
[13] USADF supports its grant making by leveraging funding from three categories of strategic partners: African governments, corporations and foundations, and other U.S. government agencies.

The lack of timely information from USADF obstructs OIG's oversight and limits visibility into the Agency's operations and programming. It also exposes taxpayer dollars and sensitive U.S. government information to significant and ongoing risks.

We prepared this management advisory from March 11, 2026, to May 15, 2026, in accordance with the *Council of the Inspectors General for Integrity and Efficiency's Quality Standards for Federal Offices of Inspectors General*. We used information from our prior reports on USADF and the status of our open recommendations.

On May 15, 2026, we issued our draft management advisory to USADF. On May 22, 2026, we received the Agency's response, which is included as an appendix to this advisory.[14] In finalizing this management advisory, we considered USADF's comments and determined that the timeline we presented in the advisory is accurate.

We appreciate USADF's ongoing assistance with our oversight work and look forward to receiving future updates from the Agency.

[14] Pursuant to Pub. L. No. 117-263 § 5274, we also provide nongovernmental organizations and businesses specifically identified in this report 30 days from the date of the report publication to submit a written response to USAID OIG. Comments received will be posted on https://oig.usaid.gov/. Please direct inquiries to oignotice_ndaa5274@oig.usaid.gov.

Appendix A. Agency Comments

Management Response to OIG advisory follow up:

Subject: OIG Management Advisory issued on May 15, 2026

Date: May 22, 2026

Executive Summary:
USADF appreciates the follow-up from the Office of Inspector General on the evaluation of our strategic partnerships and grants administration. The Agency has identified discrepancies in the timeline provided in the OIG management advisory. We would like to provide a corrected account of our operational status since February 2025.

USADF Severe Operational disruptions:

On February 21, 2025, at the direction of Mr. Peter Marocco, members of the DOGE team requested full access to USADF's IT systems, grants database, employee HR files, and all active contracts. They stated their intent to terminate all staff and active grants within two days and complete the Agency's shutdown by Monday, February 24, 2025. The DOGE team gained access to Agency systems and personnel data later that month.

On March 18, 2025, USADF employees began receiving emails from Mr. Peter Marocco informing them that their employment was terminated as part of a reduction in force (RIF), with separation dates effective April 30, 2025, and May 7, 2025.

During the same period, USADF contract personnel received termination notices, including 15 Country Program Coordinators in Africa who were responsible for local oversight activities on behalf of the Agency. As a result, USADF no longer had active personnel in Africa - either direct employees or contractors - capable of carrying out grant implementation services.

On April 8, 2025, DOGE reported the termination of all but 108 grants. These cancellations were posted publicly on the DOGE website. The Agency immediately sought clarification from the DOGE team regarding which grants remained active; however, no response was ever received. Based on available information, the Agency believes the remaining grants were canceled in June 2025.

From May 2025 through July 2025, USADF was reduced to a single active employee, who was barred by Mr. Marocco from directly engaging with stakeholders, including the OIG, Congress, and other government entities.

On July 2nd, 2025, the U.S. District Court in, *Rural Development Innovations Ltd (RDI). v. Marocco* case, issued a preliminary injunction finding that Mr. Marocco's appointment as Chair of the USADF Board was unlawful because he had not received Senate confirmation as required under 22 U.S.C. Chapter 7 § 290h. The injunction nullified all actions taken by Mr. Marocco while the litigation remained pending. The court order was shared with all Agency service providers at the Departments of the Treasury and the Interior to begin the process of reinstating staff, contracts, and grants.

By September 2025, the reinstatement process, which took approximately six to eight weeks, was fully completed, shortly before the **government shutdown** which lasted from October 1 – November 12, 2025.

On December 1, **2025**, USADF staff found that they were locked out of headquarters. An urgent inquiry to the building manager and Data Watch, the security key card vendor, revealed through counsel that Mr. Marocco had directed that all staff access be terminated. Staff received no advance notice or communication from Mr. Peter Marocco regarding the revocation of access to USADF headquarters.

On December 12, 2025, All USADF staff lost access to their official USADF emails, Treasury payment systems, files, and databases.

On December 17, 2025, Mr. Marocco signed a contract agreement with SCAR LLC valued at $954, 880. The contract was intended to provide "comprehensive services for the inventory and statutory drawdown of USADF offices both in Washington and overseas" (see attached contract). Staff both FTEs and Contractors received termination and RIF notices after SCAR LLC's takeover of Agency operations.

On January 7, 2026, Mr. Marocco began coordinating with the General Services Administration (GSA) to transfer USADF assets, including furniture and IT equipment. The first four trucks carrying Agency assets were delivered to GSA during the first week of January.

On January 13, 2026, GSA confirmed receipt of an additional eight trucks of USADF assets, which were subsequently entered into GSA inventory for transfer to other federal and DOD agencies.

On January 21, 2026, Mr. Marocco executed a second contract with SCAR LLC for an additional $362,000, significantly expanding the company's scope of work to include managing the closure of USADF financial accounts and conducting a comprehensive audit of the Agency's financial systems and record-keeping infrastructure. That addendum was later amended to provide for monthly payments of $447,120, effective March 1, 2026.

In February 2026, Mr. Marocco entered into an interagency agreement with the Export-Import Bank (EXIM) to secure two offices and storage space for the permanent relocation of USADF headquarters to EXIM premises. After the agreement was finalized, EXIM authorized Mr. Marocco and SCAR contractors to move into the new location beginning March 2, 2026.

On February 26, 2026, SCAR contractors provided 30 servers and related IT equipment to the OIG. Prior to delivery, the SCAR contractors created backups and downloaded data from the servers. The current location of these copies and servers is unknown.

In the first week of March 2026, SCAR contractors restored USADF staff member Anthony Tweneboah-Koduah's access to official email and certain Treasury systems. Mr. Tweneboah-Koduah indicated his willingness to continue assisting with the OIG audit, but SCAR contractor Patrick Martell, stated that responding to OIG document requests was unnecessary and prevented him from continuing audit-related work. OIG representatives also sought meetings with Mr. Peter Marocco and his contractors directly, though it is unclear whether those meetings occurred or what was discussed.

On March 13, 2026, the U.S. District Court issued a final ruling in *RDI v. Marocco* in favor of the plaintiff, RDI. The court found that Mr. Marocco's appointment was unlawful and held that his actions should be null and void, granting permanent relief consistent with the plaintiff's claims. In order to comply with the court order, USADF leadership began the process of reinstating operational capacity.

On April 27, 2026, and despite the District Court's ruling, only three USADF staff members had regained access to their official email accounts and resumed conducting Agency business. Senior leadership focused on compliance with the District Court's order, including restoring email access, regaining access to Treasury systems, and locating Agency assets.

On May 6, 2025, USADF staff discovered that Agency furniture and IT equipment, including servers, were stored across four separate locations: GSA, OIG, EXIM Bank, and SCAR LLC premises.

- SCAR LLC returned some items; however, no inventory list was provided, and it remains unclear whether all Agency property has been accounted for.
- GSA agreed to provide an inventory list of IT equipment but confirmed that the servers are not located on their premises. GSA further advised that some Agency property had been consolidated at its facilities, while most items were transferred to other agencies and Department of Defense components (see attached list of IT equipment).
- EXIM Bank confirmed that it maintains 6 USADF file cabinets and no additional significant Agency property.

- OIG has returned 21 of the 30 IT equipment units and legacy servers in its possession.

USADF bank accounts overseas:
Since regaining access to our official email, the Agency has reestablished communication with our points of contact with all overseas bank accounts. We have since obtained account statements confirming that $9.6 million in funds is fully accounted for. We are waiting to confirm data from two banks. In response to the IG's concerns, we will continue to monitor bank statements and continue to strengthen oversight and accountability.

USADF Financial Statement Audit:
In response to the FY 2025 Financial Statement Audit, USADF was unable to provide a certification regarding the accuracy of its financial statements and accompanying information due to the agency's shutdown. As described above, agency staff were either prevented from responding to the OIG directly or their employment was terminated by Mr. Marocco. As of May 22, USADF staff do not have access to certain Treasury systems, including PRISM and OBI due largely to the destruction of the Agency's IT systems.

USADF IT equipment:
On May 12, 2026, SCAR confirmed possession of certain USADF IT equipment and agreed to return it. According to SCAR, they had been instructed by Mr. Peter Marocco to strip the IT/server room of its equipment.

On May 14, 2026, SCAR returned some equipment, including racks, an Uninterruptible Power Supply (UPS), and several Cisco and Cisco Meraki switches. Most of the returned equipment, including the UPS units and switches, is end-of-life and no longer supported.

As stated above, OIG also confirmed possession of 30 IT assets and servers. 21 servers were subsequently collected and returned to USADF, most of which are also end-of-life and unsupported.

In summary, critical equipment remains missing, including the Verizon internet router and the agency's firewall. The returned equipment requires professional installation and integration, including the UPS power system, data and voice routers, and firewall necessary to manage and secure internet traffic. Without all required components installed and functioning together, the IT system cannot operate effectively. Acquiring, installing, and configuring a replacement system is estimated to take approximately two to three months.