

OFFICE OF INSPECTOR GENERAL

U.S. Agency for International Development

FISMA: Despite Weaknesses, USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2024

Audit Report A-ADF-24-003-C
August 29, 2024






OFFICE OF INSPECTOR GENERAL

U.S. Agency for International Development

MEMORANDUM

DATE: August 29, 2024

TO: Travis Adkins
President and Chief Executive Officer
U.S. African Development Foundation

FROM: Paul K. Martin, 
Inspector General

SUBJECT: FISMA: Despite Weaknesses, USADF Generally Implemented an Effective Information Security Program for Fiscal Year 2024 (A-ADF-24-003-C)

Enclosed is the final audit report on the U.S. African Development Foundation's (USADF) information security program for fiscal year (FY) 2024, in support of the Federal Information Security Modernization Act of 2014 (FISMA).¹ The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of RMA Associates LLC to conduct the audit. The contract required RMA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed RMA's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on USADF's compliance with FISMA. RMA is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which the audit firm did not comply, in all material respects, with applicable standards.

The audit objective was to determine whether USADF implemented an effective information security program.² To answer the audit objective, RMA assessed the effectiveness of USADF's implementation of the FY 2024 Inspector General (IG) FISMA reporting metrics that fall into the nine domains in the following table.³ Also, RMA assessed USADF's implementation of

¹ Pursuant to the Pub. L. No. 117-263 § 5274, USAID OIG provides nongovernmental organizations and/or businesses specifically identified in this report 30 days from the date of report publication to submit a written response to USAID OIG. Any comments received will be posted on <https://oig.usaid.gov/>. Please direct inquiries to oinotice_ndaa5274@usaid.gov.

² For this audit, an effective information security program is defined as having an overall mature program based on the current year IG FISMA reporting metrics.

³ Office of Management and Budget and Council of the Inspectors General on Integrity and Efficiency's "FY 2023 - 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," February 10, 2023.

applicable controls outlined in the National Institute of Standards and Technology’s Special Publication 800-53, Revision 5, “Security and Privacy Controls for Federal Information Systems and Organizations,” updated December 2020.

RMA reviewed 4 judgmentally selected systems of the 12 in USADF’s inventory as of October 10, 2023. RMA conducted its work in USADF’s headquarters located in Washington, DC, from September 15, 2023, to July 2, 2024. It covered the period from October 1, 2023, through July 2, 2024.

RMA concluded that USADF generally implemented an effective information security program. For example, USADF:

- Maintained an effective configuration management program,
- Implemented an effective incident response program,
- Maintained an effective information system continuous monitoring program,
- Implemented an effective data protection and privacy program, and
- Maintained an effective risk management program.

However, as summarized in the table below, RMA found weaknesses in five of nine IG FISMA metric domains.

Fiscal Year 2024 IG FISMA Metric Domains	Weaknesses Identified
Risk Management	
Supply Chain Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	
Security Training	X
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	X

RMA also determined that USADF took final corrective action on one recommendation from the FY2021 FISMA audit, but Agency management had not submitted a request to close it.⁴ Refer to Appendix II of RMA’s report for the status of prior year recommendations.

⁴ Recommendation I in USAID OIG, [USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA](#) (A-ADF-22-001-C), November 8, 2021.

We are making seven new recommendations. To address the weaknesses identified in the report, we recommend that USADF's Chief Information Officer take the following actions:

Recommendation 1. Develop and implement procedures to assess whether position risk designations are reviewed for all personnel.

Recommendation 2. Develop and implement procedures to assess whether reinvestigations are performed timely for individuals who possess critical-sensitive/high-risk roles that require system access.

Recommendation 3. Develop and implement policies and procedures to periodically assess its cybersecurity workforce's knowledge, skills, and abilities to confirm that security training and development activities align with agency needs.

Recommendation 4. Develop and implement policies and procedures for agency personnel to monitor performance metrics for information technology services provided by third parties.

Recommendation 5. Update the change management charter to designate in writing the responsibilities for monitoring performance metrics, conducting lessons-learned activities, and documenting routine updates and minor changes.

Recommendation 6. Update the system security plan to include the frequency for reviewing and updating the contingency plan.

Recommendation 7. Develop and implement policies and procedures to obtain feedback on the agency's specialized security training, update the training program, and request that third-party providers update their training content, as appropriate, to keep current with security practices.

In finalizing the report, RMA evaluated USADF's responses to the recommendations. After reviewing that evaluation, we consider all seven recommendations resolved but open pending completion of planned activities. Please provide evidence of final action to OIGAuditTracking@usaid.gov.

We appreciate the assistance provided to our staff and the audit firm's employees during the engagement.



U.S African Development Foundation
(USADF)
Federal Information Security Modernization Act of 2014
(FISMA)
Final Report
Fiscal Year 2024



August 26, 2024

Ms. Lisa Banks
Director, Information Technology Audits Division
United States Agency for International Development
Office of the Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20005-2221

Dear Ms. Banks:

The independent certified public accounting firm, RMA Associates, LLC, is pleased to present our report on the United States African Development Foundation (USADF) compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024.

Thank you for the opportunity to serve your organization and the assistance provided by your staff and that of USADF. We will be happy to answer any questions you may have concerning the report.

Thank you,

A handwritten signature in black ink that reads "Reza Mahbod". The signature is written in a cursive style.

Reza Mahbod, CPA, CISA, CGFM, CICA, CGMA, CDFM, CFE, CDPSE
President
RMA Associates, LLC



Inspector General
United States Agency for International Development
Washington, D.C.

August 26, 2024

RMA Associates, LLC, conducted a performance audit of the United States African Development Foundation's (USADF) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether USADF implemented an effective information security program. The scope of this audit was to assess USADF's information security program consistent with FISMA and reporting instructions issued by the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency. The audit included tests of management, technical, and operational controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, updated December of 2020.

For this audit, we reviewed four of twelve judgmentally selected systems in USADF's inventory as of October 10, 2023. Our work covered USADF's headquarters located in Washington, DC, from September 15, 2023, to July 2, 2024.

Our audit was performed in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We concluded that USADF generally implemented an effective information security program based on USADF's overall implementation of security controls and considering the unique mission, resources, and challenges of USADF. However, we found weaknesses in USADF's security posture in preserving the agency's information and information systems' confidentiality, integrity, and availability. Consequently, we noted weaknesses in five of the nine Inspector General FISMA Metric Domains. We made seven recommendations to assist USADF in strengthening its information security program.

Additional information on our findings and recommendations are included in the accompanying report.

Respectfully,

A handwritten signature in blue ink that reads 'RMA Associates' in a cursive, slightly stylized font.

RMA Associates LLC

Table of Contents

Summary of Results	1
Background.....	1
Audit Results	2
Audit Findings.....	5
1. USADF Did Not Periodically Review Personnel Risk Designations and Rescreen Personnel Who Possess Critical-Sensitive/High-Risk Roles with System Access.....	5
2. USADF Did Not Perform an Assessment of the Knowledge, Skills, and Abilities of its Cybersecurity Workforce to Tailor Security Specialized Training.....	6
3. USADF Did Not Monitor the Performance Metrics Tied to Supply Chain Risk Management Services from Third-Parties.....	7
4. USADF Did Not Fully Implement Controls for Change Management Activities.....	8
5. USADF Needs to Update Its Contingency Plan to Include the Most Recent Documentation for all Contingency Plan Activities.....	9
6. USADF Did Not Request Feedback on the Specialized Security Training Content and Program.....	10
Evaluation of Management Comments	12
Appendix I – Scope and Methodology	13
Scope	13
Methodology	13
Appendix II – Status of Prior Year Recommendations	15
Appendix III – USADF Management’s Comments	16

Summary of Results

Background

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) engaged RMA Associates, LLC (RMA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014¹ (FISMA) requirement for an evaluation of the United States African Development Foundation's (USADF) information security program for fiscal year (FY) 2024. The objective of this performance audit was to determine whether USADF implemented an effective information security program.²

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. 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 also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes.

FISMA also requires the agency Inspectors General (IGs) to assess the effectiveness of agency information security programs and practices and report the results of the assessments to the Office of Management and Budget. The FY 2024 metrics are designed to assess the maturity³ of an information security program and align with the five functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1.

¹ The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

² For this audit, an effective information security program is defined as having an overall mature program based on the current year Inspector General FISMA reporting metrics.

³ The five maturity levels are: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2024 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Audit Results

This audit was performed in accordance with generally accepted government auditing standards. RMA determined the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objective.

The audit concluded that USADF generally implemented an effective information security program. For example, USADF:

- Maintained an effective configuration management program,
- Implemented an effective incident response program,
- Maintained an effective information system continuous monitoring program,
- Implemented an effective data protection and privacy program, and
- Maintained an effective risk management program.

As shown in Table 2, the overall maturity of USADF's information security program was Managed and Measurable (Effective).

Table 2: FY 2024 USADF Maturity Level

Cybersecurity Framework Security Functions	Core Metric	FY 24 Supplemental Metric	FY 24 Assessed Maturity Level
Identify	Effective	Effective	Managed and Measurable
Protect	Effective	Ineffective	Consistently Implemented
Detect	Effective	Effective	Managed and Measurable
Respond	Effective	Effective	Optimized
Recover	Effective	Ineffective	Managed and Measurable
Overall	Effective	Ineffective	Managed and Measurable

However, we found weaknesses in USADF's security posture in preserving its information and information systems' confidentiality, integrity, and availability. As a result, we noted weaknesses in five of the nine IG FISMA Metric Domains (Table 3) and presented recommendations to strengthen the agency's information security program.

Table 3: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2024 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains	FY 2024 Weakness Noted
Identify	Risk Management	None
	Supply Chain Risk Management	USADF Did Not Monitor Performance Metrics Tied to Supply Chain Risk Management Services from Third-Parties (Finding 3)
Protect	Configuration Management	USADF Did Not Fully Implement Controls for Change Management Activities (Finding 4)
	Identity and Access Management	USADF Did Not Periodically Review Personnel Risk Designations and Rescreen Personnel Who Possess Critical-Sensitive/High-Risk Roles with System Access (Finding 1)
	Data Protection and Privacy	None
	Security Training	USADF Did Not Perform an Assessment of the Knowledge, Skills, and Abilities of its Workforce to Tailor Specialized Security Training (Finding 2) USADF Did Not Request Feedback on the Specialized Security Training Content and Program (Finding 6)
Detect	Information Security Continuous Monitoring	None
Respond	Incident Response	None
Recover	Contingency Planning	USADF Needs to Update Its Contingency Plan to Include the Most Recent Documentation for all Contingency Plan Activities (Finding 5)

We are making seven new recommendations to address the weaknesses. In addition, USADF took corrective action to address one open recommendation from the FY 2021 FISMA audit, but USADF has yet to provide an official closure request for processing. (See Appendix II)

Audit Findings

1. USADF Did Not Periodically Review Personnel Risk Designations and Rescreen Personnel Who Possess Critical-Sensitive/High-Risk Roles with System Access.

Cybersecurity Framework Security Function: *Protect*

FY24 IG FISMA Metric Domain: *Identity and Access Management*

On an annual basis, USADF performs an access review of all system users. However, within the annual review, USADF did not make considerations for critical-sensitive/high-risk designations or status of security investigations for individuals with critical-sensitive/high-risk roles with system access. Two individuals with critical-sensitive/high-risk roles had not been reinvestigated within the last five years as required.

United States African Development Foundation (USADF) Information Technology Security Implementation Handbook states:

Position Risk Designation (PS-2)

...

Position risk designations shall be reviewed at least every three years by OHR in conjunction with the individuals' managers/supervisors requiring access. Investigation types (e.g., NACI, SSBI, etc.) held by personnel must be reviewed annually by the ISSO against the positions these personnel currently occupy to ensure the investigation type conducted matches their current position.

System Owners, Project Managers, or Contracting Officer's Technical Representative (COTR) shall be responsible for reviewing the investigation type for contractors annually.

Personnel Screening (PS-3)

All individuals requiring access to USADF information and information systems must be screened before their access authorization has been granted.

Screening shall be consistent with the Office of Personnel Management (OPM) Classifier Handbook and 5 CFR (Code of Federal Regulations) Part 731, Suitability.

The Code of Federal Regulations, Title 5, Chapter 1, Part 731, Subpart A, Section 731.106 Designation of public trust positions and investigative requirements, states:

(d) Reinvestigation requirements.

(1) Agencies must ensure that reinvestigations are conducted, and a determination made regarding continued employment of persons occupying public trust positions at least once every 5 years. The nature of these reinvestigations and any additional requirements and parameters will be established in supplemental guidance issued by OPM.

Although USADF relied on the Department of the Interior for assigning risk designations and periodically rescreening personnel, the agency did not have procedures in their annual review process to ensure position risk designations were reviewed for all personnel and that reinvestigations were performed timely for individuals who possess critical-sensitive/high-risk roles that required system access. During the assessment, USADF concluded that their personnel were subject to continuous vetting and continuous evaluation through the Continuous Vetting for Non-Sensitive Public Trust positions; however, this did not apply to the two individuals identified. Further, USADF deemed this a low-risk activity since the access was related to a system which is categorized as a low security impact system. As a result, individuals may have improper system access that may require change or disablement. Therefore, we are making the following recommendations.

Recommendation 1: *We recommend that USADF's Chief Information Officer develop and implement procedures to assess whether position risk designations are reviewed for all personnel.*

Recommendation 2: *We recommend that USADF's Chief Information Officer develop and implement procedures to assess whether reinvestigations are performed timely for individuals who possess critical-sensitive/high-risk roles that require system access.*

2. USADF Did Not Perform an Assessment of the Knowledge, Skills, and Abilities of its Cybersecurity Workforce to Tailor Specialized Security Training.

Cybersecurity Framework Security Function: *Protect*
FY24 IG FISMA Metric Domain: *Security Training*

USADF officials periodically updated its *Security and Awareness Training Policy* to adapt to a changing risk environment. However, USADF did not assess whether there were gaps in its cybersecurity workforce's knowledge, skills, and abilities. Consequently, they did not revise the specialized training to address these potential gaps.

The Federal Cybersecurity Workforce Assessment Act of 2015, Section 3, titled National Cybersecurity Workforce Measurement Initiative states the following:

- (a) In General.—The head of each Federal agency shall—
 - (1) identify all positions within the agency that require the performance of information technology, cybersecurity, or other cyber-related functions; and
 - (2) assign the corresponding employment code, which shall be added to the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework, in accordance with subsection

The NIST SP 800-181, Revision 1, Workforce Framework for Cybersecurity (NICE Cybersecurity Workforce Framework) is the guidance for fulfilling Federal Cybersecurity Workforce Assessment, and it states:

The Workforce Framework for Cybersecurity (NICE Framework) is built upon a set of discrete building blocks that describe the work to be done (in the form of Tasks) and what is required to perform that work (through Knowledge and Skills). These building blocks are organizing constructs that support the usability and implementation of the NICE Framework. They provide a mechanism by which both organizations and individuals can understand the scope and content of the NICE Framework.

...

The NICE Framework helps guide the efforts of employers to describe cybersecurity work, education and training providers to prepare cybersecurity workers, and learners to demonstrate their capabilities to perform cybersecurity work.

USADF did not have policies and procedures to ensure the assessment was completed. According to USADF officials, the agency is small and has a limited cybersecurity workforce of 4-5 employees. Therefore, the official did not consider it beneficial to conduct formal workforce assessments. However, because there was no systematic evaluation of the cybersecurity workforce's competencies, USADF did not have assurance that the training was effective and comprehensive. This puts USADF at risk that could lead to vulnerabilities in USADF security posture due to unaddressed deficiencies in staff capabilities. Therefore, we are making the following recommendation.

Recommendation 3: *We recommend that USADF's Chief Information Officer develop and implement policies and procedures to periodically assess its cybersecurity workforce's knowledge, skills, and abilities to confirm that security training and development activities align with agency needs.*

3. USADF Did Not Monitor the Performance Metrics Tied to Supply Chain Risk Management Services from Third-Parties.

Cybersecurity Framework Security Function: *Identify*

FY24 IG FISMA Metric Domain(s): *Supply Chain Risk Management*

USADF did not monitor qualitative and quantitative performance metrics for the performance of third parties' supply chain risk management (SCRM) services.

NIST SP 800-55, Revision 1, Performance Measurement Guide for Information Security states:

5.5.3 Establishing Performance Targets

Establishing performance targets is an important component of defining information security measures. Performance targets establish a benchmark by which success is measured. The degree of success is based on the proximity of the measure result to the stated performance target. The mechanics of establishing performance targets differ for implementation measures and the other two types of

measures (effectiveness/efficiency and impact). For implementation measures, targets are set to 100 percent completion of specific tasks.

USADF did not have policies and procedures for agency personnel to monitor performance metrics for information technology services provided by third parties. According to USADF officials, USADF outsourced procurement activities and was under the impression that no ongoing monitoring was required because the Bureau of Fiscal Service ensures all contract requirements were met in accordance with SCRM. However, according to FISMA:

Each agency shall develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Therefore, USADF was responsible for assuring that the services provided by the Bureau of Fiscal Services met SCRM requirements. Because USADF did not monitor SCRM performance metrics, the agency has no insight to whether its supply chain was compromised, affecting the confidentiality, integrity, and availability of its information and information systems. Therefore, we are making the following recommendation.

***Recommendation 4:** We recommend that USADF's Chief Information Officer develop and implement policies and procedures for agency personnel to monitor performance metrics for information technology services provided by third parties.*

4. USADF Did Not Fully Implement Controls for Change Management Activities.

Cybersecurity Framework Security Function: *Protect*

FY24 IG FISMA Metric Domain: *Configuration Management*

USADF did not follow its change management process in accordance with the USADF Change Management Charter. Specifically, USADF did not document changes for routine updates and minor changes that occurred. In addition, USADF did not monitor performance metrics to assess the effectiveness of change management activities. Further, USADF's personnel did not assess lessons learned to improve its change management activities accordingly.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, states:

CM-3 Configuration Change Control

Control: The organization

...

f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].

In addition, NIST Special Publication 800-55 Revision 1 *Performance Measurement Guide for Information Security* (July 2008) states:

3.5 Information Security Measurement Program Scope

An information security measurement program can be scoped to a variety of environments and needs:

- Quantifying information system-level security performance for an information system;
- Quantifying the integration of information security into the s cycle (SDLC) during the information system and software development process and
- Quantifying enterprise-wide information security performance.

According to USADF management, routine updates and minor changes did not require adherence to the formal change management process within the USADF Change Management Charter. However, the charter did not specify any exceptions for bypassing the change management process. Moreover, the responsibilities of monitoring performance metrics, developing lessons learned, and documenting routine updates and minor changes were not assigned in the charter. As a result, there was no information to improve the change management process in the USADF Change Management Charter. Therefore, we are making the following recommendation.

Recommendation 5: *We recommend that USADF's Chief Information Officer update the change management charter to designate in writing the responsibilities of monitoring performance metrics, conducting lessons-learned activities, and documenting routine updates and minor changes.*

5. USADF Needs to Update Its Contingency Plan to Include the Most Recent Documentation for all Contingency Plan Activities.

Cybersecurity Framework Security Function: *Recover*

FY24 IG FISMA Metric Domain: *Contingency Planning*

USADF's contingency planning development and maintenance activities were not fully updated with other continuity activities. Specifically, USADF leveraged a third-party service provider's Disaster Recovery Plan, but that plan has not been updated since July 15, 2013. In addition, USADF officials did not update the embedded hyperlinks in the external service provider's documentation.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* states:

CP-2 Contingency Plan

Control: The organization...

- d. Review the contingency plan for the system [Assignment: organization-defined frequency];
- e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

USADF became over-reliant on its third-party provider services and inherited controls. Thus, USADF did not review its contingency plan or define the frequency of conducting such reviews in its system security plan. As a result, in the event of an emergency, USADF personnel are at risk of referencing out-of-date or inaccurate information. This may lead to a delayed response in certain situations and prolonged downtime for agency operations. Further, employees may not know how to react in a timely manner to recover agency operations. Therefore, we are making the following recommendation.

***Recommendation 6:** We recommend that USADF's Chief Information Officer update the system security plan to include the frequency for reviewing and updating the contingency plan.*

6. USADF Did Not Request Feedback on the Specialized Security Training Content and Program.

Cybersecurity Framework Security Function: *Protect*
FY24 IG FISMA Metric Domain: *Security Training*

USADF did not request participant feedback on the specialized security training content, nor did it require consideration of feedback toward updates to its training program or third-party content.

NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations states:

AT-6 Training Feedback

Control: The organization

Provide feedback on organizational training results to the following personnel [Assignment: organization-defined personnel].

...

Training feedback supports the evaluation and update of organizational training...

In prior years, USADF was reliant on third-party training providers to obtain feedback to improve training sessions. Upon being made aware of this requirement by RMA auditors, USADF obtained feedback from its personnel and provided it after the auditors' due date. Nonetheless, USADF did not initially receive feedback because it lacked policies and procedures requiring solicitation of feedback from personnel. This feedback may be used to update the specialized security training program or request additional content from third-party providers. As a result, USADF is at risk that its specialized training may not keep personnel up to date with current security practices, leaving the agency vulnerable to unauthorized disclosure or alteration of information or information systems. Therefore, we are making the following recommendation.

Recommendation 7: *We recommend that USADF's Chief Information Officer develop and implement policies and procedures to obtain feedback on its specialized security training, update the training program, and request that third-party providers update their training content, as appropriate, to keep current with security practices.*

Evaluation of Management Comments

In response to the draft report, USADF outlined its plan to address each of the seven recommendations. USADF's comments are included in their entirety in Appendix III. Based on our evaluation of management comments, we acknowledge management's decision on each of the seven recommendations. Further, the recommendations are open pending the completion of planned activities.

Appendix I – Scope and Methodology

Scope

RMA conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our audit was conducted for FY 2024 and tested the core and supplemental metrics identified in the *FY 2023-2024 IG FISMA Reporting Metrics* issued by the Department of Homeland Security (DHS).

The scope of this audit was to assess USADF's information security program consistent with FISMA and reporting instructions issued by the Office of Management and Budget and DHS. In addition, the audit included tests of management, technical, and operational controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* dated December 10, 2020. We assessed USADF's performance and compliance with FISMA in the following control areas:

- Risk Management
- Supply Chain Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Awareness Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning

For this audit, we reviewed four of twelve systems in USADF's inventory as of October 10, 2023. The audit also included a follow-up on one prior audit recommendation⁴ to determine if USADF had made progress in implementing the recommended improvements concerning its information security program. See Appendix II for the status of recommendations for the prior year.

Our work was conducted at USADF's headquarters located in Washington, DC, from September 15, 2023, to July 2, 2024. It covered the period from October 1, 2023, through July 2, 2024.

Methodology

To determine if USADF implemented an effective information security program, RMA conducted interviews with USADF officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. Additionally, RMA reviewed documentation supporting the information security program. These documents included, but were not limited to, USADF's (1) risk management policy; (2) configuration management

⁴ Recommendation 1 in *USADF Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report No. A-ADF-22-001-C November 8, 2021).

procedures; (3) identity and access control measures; (4) security awareness training; and (5) continuous monitoring controls. RMA compared documentation against requirements stipulated in NIST special publications. Also, RMA performed tests of information system controls, including a vulnerability assessment, to determine the effectiveness of those controls. Furthermore, RMA reviewed the status of FISMA audit recommendations for FY 2021.

In testing the effectiveness of the security controls, RMA exercised professional judgment in determining the number of items selected for testing and the method used to select them. RMA considered the relative risk and the significance of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the proportion of deficient items found compared to the total population available for review when documenting the results of our testing. Lastly, in some instances, RMA tested samples rather than the entire audit population. In those cases, the results cannot be projected to the population as that may be misleading.

Appendix II – Status of Prior Year Recommendations

The following table provides the status of the FY 2021 FISMA audit recommendations.

Table 4: FY 2021 FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2021 Audit Recommendations	USADF's Corrective Action	USADF's Position	Auditor's Position on the Status
A-ADF-22-001-C (Rec.1)	We recommend that USADF's Chief Information Security Officer formally document and implement a process for validating that medium and low-risk vulnerabilities are remediated in accordance with the agency's policy.	USADF updated its policy, which now says that medium and low-risk vulnerabilities must be addressed as time permits at the discretion of the Chief Information Security Officer (CISO).	Closed, but USADF did not submit a closure request	Closed after USADF submits its official closure request.

Appendix III – USADF Management's Comments

August 20, 2024



Mrs. Gabriele Tonsil

Deputy Assistant Inspector General for Audit

USAID, Office of the Inspector General

1300 Pennsylvania Avenue, NW

Washington, DC 20523

Subject: Audit of the United States African Development Foundation (USADF):
Response to the Draft Evaluation Report on USADF's Compliance with FISMA for FY24
(Report No. A-ADF-24-00X-C)

Dear Mrs. Tonsil:

This letter responds to the findings presented in your above-captioned draft report. We appreciate your staff's efforts in working with us to improve the Foundation's information security program and compliance with the provisions of the Federal Information Security Management Act of 2014 and NIST SP 800-53. We have reviewed your report and have the following comments in response to your recommendations.

1. USADF Did Not Periodically Review Personnel Risk Designations and rescreen personnel who possess critical-sensitive/high-risk roles with system access

Cybersecurity Framework Security Function: *Protect*

FY24 IG FISMA Metric Domain: *Identity and Access Management*

Recommendation 1: *We recommend that USADF's Chief Information Officer develop and implement procedures to assess whether position risk designations are reviewed for all personnel.*

Management Response:

USADF's General Support System (GSS) only requires Sensitive But Unclassified (SBU) access. Thus, USADF information systems have a public trust designation

and classification. Consequently, access to critical-sensitive/high-risk systems is not required with USADF's GSS. Furthermore, the Interior Business Center (IBC) of the Department of Interior, as USADF's shared services provider, conducts USADF's personnel risk assessment and designation. However, USADF will develop a plan to reinforce its oversight of the activities to ensure IBC conducts the personnel risk assessment and designation by the current Office Personnel Management (OPM) Memorandum dated October 3, 2023. Corrective action is expected to be completed by November 30th, 2024.

Recommendation 2: We recommend that USADF's Chief Information Officer develop and implement procedures to assess whether reinvestigations are performed timely for individuals who possess critical-sensitive/high-risk roles that require system access.

Management Response: All information systems at USADF have a public trust designation and classification. Those who possess critical-sensitive/high risk roles are for access to other federal agencies with such classification requiring access. Procedures for access are controlled by those agencies' security personnel and not USADF.

The Interior Business Center (IBC) of the Department of Interior, as USADF's shared services provider, conducts USADF's personnel risk assessment, designation, and re-investigations. USADF will develop a plan to reinforce its oversight of the activities to ensure IBC conducts the personnel risk assessment and designation by the current Office Personnel Management (OPM) Memorandum dated October 3, 2023. Corrective action is expected to be completed by November 30th, 2024.

2. USADF Did Not Perform an Assessment of the Knowledge, Skills, and Abilities of its Cybersecurity Workforce to tailor security specialized training.

Cybersecurity Framework Security Function: *Protect*

FY24 IG FISMA Metric Domain: *Security Training*

Recommendation 3: We recommend that USADF's Chief Information Officer develop and implement policies and procedures to periodically assess its cybersecurity workforce's knowledge, skills, and abilities to confirm that security training and development activities align with agency needs.

Management Response:

We understand the finding and want to clarify that we conducted an assessment required by DHS annually in Cyberscope and generates a report . A workforce assessment was completed following the NICE framework (NIST SP 800-181 Rev.1) report was generated and submitted to the auditors. We feel we have met the requirements, but we acknowledge that this was not accepted. Therefore, we will develop and implement new procedure as recommended by the finding and according to the Federal Cybersecurity Framework. The completion of these policies and procedures is expected by March 15th, 2025.

However, USADF will proactively update its policies and procedures based on the audit recommendation by March 15, 2025, demonstrating our unwavering commitment to compliance.

3. USADF Did Not Monitor the Performance Metrics Tied to Supply Chain Risk Management Services from Third Parties.

Cybersecurity Framework Security Function: *Identify*

FY24 IG FISMA Metric Domain(s): *Supply Chain Risk Management*

Recommendation 4: *We recommend that USADF's Chief Information Officer develop and implement policies and procedures for agency personnel to monitor performance metrics for information technology services provided by third parties.*

Management Response: As part of the Interagency Agreement (IAA) between USADF and the Bureau of the Fiscal Service (BFS), quarterly performance metrics for technology services are provided by BFS reports for ADF. These performance metrics monitoring reports will be made available with the closing memo for this finding. USADF recommends closing of this finding when the closing memo is submitted on October 15th, 2024.

4. USADF Did Not Fully Implement Controls for Change Management Activities

Cybersecurity Framework Security Function: *Protect*

FY24 IG FISMA Metric Domain: *Configuration Management*

Recommendation 5: *We recommend that USADF's Chief Information Officer update the change management charter to designate in writing the responsibilities of monitoring performance metrics, conducting lessons-learned activities, and documenting routine updates and minor changes.*

Management Response:

We accept the recommendation that the USADF Chief Information Officer update the change management charter to designate the responsibilities of monitoring performance metrics, conducting lessons-learned activities, and documenting routine updates and minor changes. In addition to these updates, USADF will update its processes to supplement the changes to the made charter. USADF expects to complete the corrective action for this recommendation by February 28th, 2025.

5. USADF Needs to Update Its Contingency Plan to Include the Most Recent Documentation for all Contingency Plan Activities.

Cybersecurity Framework Security Function: *Recover*

FY24 IG FISMA Metric Domain: *Contingency Planning*

Recommendation 6: *We recommend that USADF's Chief Information Officer update the system security plan to include the frequency for reviewing and updating the contingency plan.*

Management Response:

USADF accepts the recommendation that the USADF Chief Information Officer update the system security plan to include the frequency of reviewing and updating the contingency plan. USADF has already made the update on March 28th and communicated to the auditors during the audit on same date. USADF will submit a corrective action memo with the updated contingency plan and recommending closure of this finding by October 31st, 2024.

6. USADF Did Not Request Feedback on the Specialized Security Training Content and Program.

Cybersecurity Framework Security Function: *Protect*

FY24 IG FISMA Metric Domain: *Security Training*

Recommendation 7: *We recommend that USADF's Chief Information Officer develop and implement policies and procedures to obtain feedback on its specialized security training, update the training program, and request that third-party providers update their training content, as appropriate, to keep current with security practices.*

Management Response:

USADF accepts the recommendation that the USADF Chief Information Officer implement policies and procedures to obtain feedback on its specialized security training, update the training program, and request that third-party providers update their training content, as appropriate, to keep current with security practices.

USADF has already implemented some aspects of the corrective action on April 30th; and communicated them to the auditors on June 7th, 2024 during the audit. The following actions are for USADF to implement the updated policies and procedures and obtain evaluation feedback. USADF reaffirms its commitment to completing this implementation phase by December 30th, 2024.

/s/

Mathieu Zahui

CFO and Managing Director, Finance

Travis Adkins, President and CEO

Cc: Solomon Chi, Chief Information Security Officer

Ellen Teel, Senior Auditor