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

USADF Implemented an Optimized Information Security Program for Fiscal Year 2022 in Support of FISMA

Report A-ADF-22-008-C
September 12, 2022

Information Technology Audits Division

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

MEMORANDUM

DATE: September 12, 2022

TO: USADF, President and Chief Executive Officer, Travis Adkins

FROM: Deputy Assistant Inspector General for Audit, Alvin Brown /s/

SUBJECT: USADF Implemented an Optimized Information Security Program for Fiscal Year 2022 in Support of FISMA (A-ADF-22-008-C)

Enclosed is the final report on the evaluation of U.S. African Development Foundation's (USADF's) information security program for fiscal year 2022, in support of the Federal Information Security Modernization Act of 2014 (FISMA). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the evaluation. The contract required the firm to perform the evaluation in accordance with the Quality Standards for Inspection and Evaluation, from the Council of the Inspectors General on Integrity and Efficiency.

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

The objective of the evaluation was to determine the maturity level that USADF achieved for each of its core FISMA reporting metrics.[1] Therefore, this evaluation was not designed to determine causes of, effects of, or recommendations to improve the maturity levels.

To answer the evaluation objective, CLA evaluated the maturity level of USADF's implementation of the 20 core metrics. The scope of the evaluation was to assess USADF's information security program consistent with reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security.[2] Also, CLA assessed USADF's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 5, *Security and Privacy Controls for*

[1] For this evaluation, "core metrics" were defined as the FY2022 inspector general FISMA reporting metrics issued by the Office of Management and Budget, Office of the Federal Chief Information Officer, "FY22 Core IG Metrics Implementation Analysis and Guidelines," April 13, 2022.
[2] FY 2022 Core IG FISMA Metrics Evaluation Guide.

Information Systems and Organizations. CLA reviewed 3 of the 11 information systems in USADF's inventory as of February 16, 2022. Evaluation fieldwork covered USADF's headquarters located in Washington, DC. Fieldwork was performed from March 30, 2022, through July 7, 2022, and covered the period from October 1, 2021, through July 7, 2022.

CLA concluded that, for the 20 core metrics, USADF's information security program was optimized for 11 metrics, managed and measurable for 4 metrics, consistently implemented for 3 metrics, defined for 1 metric, and ad hoc for 1 metric. Therefore, USADF's information security program was calculated as optimized.

USADF management agreed with the report's conclusions and provided updates on the status of prior recommendations. The report does not include recommendations.

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

U. S. African Development Foundation
Federal Information Security Modernization Act of 2014
Evaluation

Fiscal Year 2022

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
CLAconnect.com

September 9, 2022

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:

CliftonLarsonAllen LLP (CLA) is pleased to present our final report on the results of our evaluation of the United States African Development Foundation's (USADF) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2022.

We appreciate the assistance we received from USADF. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
United States Agency for International Development

CliftonLarsonAllen LLP (CLA) conducted an evaluation of the United States African Development Foundation's (USADF) information security program and practices for Fiscal Year (FY) 2022 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an Agency-wide information security program and practices. The Act also requires Inspectors General (IGs) to conduct an annual review of their agencies' information security program and report the results to the Office of Management and Budget (OMB).

The objective of this evaluation was to determine what maturity level USADF achieved for each of its Core IG metrics. For this evaluation, "Core metrics" are defined as the OMB Office of the Federal Chief Information Officer *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (FY 2022 Core Metrics).

For this year's review, OMB required IGs to assess 20 Core Metrics in the following five security function areas to assess the maturity level and the effectiveness of their agencies' information security program: Identify, Protect, Detect, Respond, and Recover. The maturity levels ranging from lowest to highest are Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. According to the FY 2022 Core Metrics, Managed and Measurable and Optimized are considered effective maturity levels.

The evaluation included an assessment of USADF's information security program and practices consistent with FISMA and reporting instructions issued by OMB. The scope also included assessing selected security controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for a sample of 3 of 11 internal and external systems in USADF's FISMA inventory of information systems.

Evaluation fieldwork covered USADF's headquarters located in Washington, DC, from March 28, 2022, to July 7, 2022. It covered the period from October 1, 2021, through July 7, 2022.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

We concluded that, for the 20 FY 2022 Core Metrics, USADF's information security program was:

- Optimized for 11 metrics.
- Managed and measurable for 4 metrics.
- Consistently implemented for 3 metrics.
- Defined for 1 metric.
- Ad Hoc for 1 metric.

CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer.

Therefore, USADF's information security program was calculated by CyberScope as Optimized.

In addition, we noted two recommendations in a prior year FISMA audit related to the FY 2022 Core Metrics. One remains open and the other is closed.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our evaluation to future periods is subject to the risks that conditions may materially change from their status. The information included in this report was obtained from USADF on or before September 9, 2022. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 9, 2022

The purpose of this evaluation report is to report on our evaluation of USADF's compliance with FISMA and is not suitable for any other purpose.

Additional information on our evaluation results is included in the accompanying report. We are submitting this report to the USAID Office of Inspector General.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
September 9, 2022

TABLE OF CONTENTS

Summary of Results 1

Evaluation Results 5

1. USADF's Implementation of 5 of 20 FY 2022 Core Metrics Was Below Managed and Measurable 5

2. USADF's Implementation of 15 of 20 FY 2022 Core Metrics Was No Less Than Managed and Measurable 6

Evaluation of Management Comments 8

Appendix I – Objective, Scope, and Methodology 9

Appendix II – Management Comments 11

Appendix III – Summary of Results for Each Core Metric 13

Appendix IV – Status of Prior Year Recommendations 23

SUMMARY OF RESULTS

Background

The United States Agency for International Development (USAID) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct an evaluation in support of the Federal Information Security Modernization Act of 2014 (FISMA) requirement for an annual evaluation of the USADF's information security program and practices. The objective of this evaluation was to determine what maturity level USADF achieved for each of its Core Inspectors General (IG) metrics. For this evaluation, "Core metrics" are defined as the Office of Management and Budget (OMB) Office of the Federal Chief Information Officer *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (FY 2022 Core Metrics). Therefore, this evaluation was not designed to determine causes of, effects of, or recommendations to improve the maturity levels.

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 source.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure that (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 agency Inspectors General (IGs) to assess the effectiveness of their respective agency's information security programs and practices. OMB and the National Institute of Standards and Technology (NIST) have issued guidance for Federal agencies to follow for implementing information security and privacy programs.

OMB and the Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On December 6, 2021, OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete IG FISMA reporting metrics[1] to independently assess their agencies' information security program. OMB selected a core group of 20 metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will be evaluated in metrics on a two-year cycle. In addition, OMB shifted the due date of the IG FISMA Reporting Metrics from October to July to better align with the release of the President's budget.[2]

---

[1] We submitted our responses to the FY 2022 Core Metrics to USAID OIG as a separate deliverable under the contract for this evaluation.

[2] OMB M-22-05 *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, December 6, 2021.

For FY 2022, OMB required IGs to assess the 20 Core Metrics in the five security function areas to assess the maturity level and effectiveness of their agency's information security program. As highlighted in Table 1, the metrics were designed to assess the maturity of the information security program and align with the five function areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover. Table 2 defines each maturity level.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2022 Metrics Domains

Cybersecurity Framework Security Functions	FY 2022 Metrics 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 (ISCM)
Respond	Incident Response
Recover	Contingency Planning

Table 2: Maturity Level Definitions

Maturity Level	Maturity Level Description[3]
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner. Achieving this maturity level is not effective.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented. Achieving this maturity level is not effective.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking. Achieving this maturity level is not effective.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes. Achieving this maturity level is effective.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs. Achieving this maturity level is effective.

[3] The FY 2022 Core Metrics define which maturity levels are effective.

For this evaluation, we reviewed selected controls[4] mapped to the FY 2022 Core Metrics for a sample of 3 of 11 internal and external information systems[5] in USADF's FISMA inventory as of February 16, 2022.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Evaluation Conclusion

CLA concluded that, for the 20 FY 2022 Core Metrics, USADF's information security program was:

- Optimized for 11 metrics.
- Managed and measurable for 4 metrics.
- Consistently implemented for 3 metrics.
- Defined for 1 metric.
- Ad Hoc for 1 metric.

Therefore, USADF's information security program was calculated by CyberScope as Optimized.[6] Table 3 below shows a summary of the overall maturity levels for each domain and function area in the FY 2022 Core Metrics.

Table 3: Maturity Levels for the FY 2022 Core Metrics

Security Function	Maturity Level by Function	Metric Domains	Maturity Level by Domain
Identify	Optimized	**Risk Management**	Optimized
		Supply Chain Risk Management	Defined
Protect	Optimized	**Configuration Management**	Managed and Measurable
		Identity and Access Management	Optimized
		Data Protection and Privacy	Optimized
		Security Training	Optimized
Detect	Optimized	**Information Security Continuous Monitoring**	Optimized
Respond	Optimized	**Incident Response**	Optimized
Recover	Managed and Measurable	**Contingency Planning**	Managed and Measurable
Overall	**Level 5: Optimized**		

[4] The controls were tested to the extent necessary to determine whether USADF implemented the processes specifically addressed in the FY 2022 Core Metrics. In addition, not all controls were tested for all three sampled information systems since several controls were inherited from the USADF general support system and certain controls were not applicable for external systems.

[5] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[6] In accordance with the FY 2022 Core Metrics, ratings throughout the nine domains were determined by a simple majority, where the most frequent level across the metrics served as the domain rating. Agencies were rated at the higher level in instances when two or more levels were the most frequently rated. The domain ratings inform the overall function ratings, and the five function ratings inform the overall agency rating.

In addition, we noted two recommendations in a prior year FISMA audit[7] related to the FY 2022 Core Metrics. One remains open, and the other is closed.[8]

In response to the draft report, USADF agreed with the evaluation results for the FY 2022 Core Metrics and provided a status of prior recommendations. USADF's comments are included in their entirety in Appendix II.

The following section discusses the evaluation results in more detail related to USADF's implementation of each FY 2022 Core Metrics by maturity level. **Appendix I** describes the evaluation objective, scope, and methodology. See **Appendix III** for a summary of results for each FY 2022 Core Metrics. **Appendix IV** includes details regarding the prior FISMA recommendations.

[7] Recommendations 1 and 2 in OIG's "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).

[8] For this evaluation we reviewed prior year recommendation closures that tied to the FY 2022 Core Metrics. The remaining prior year recommendation closures will be reviewed at a later time.

EVALUATION RESULTS

1. USADF's Implementation of 5 of 20 FY 2022 Core Metrics was Below Managed and Measurable

USADF's implementation of metrics 10, 14, 21, 32, and 63 was below Managed and Measurable (Level 4). The following paragraphs discuss each in detail.

Ad Hoc (Level 1) - USADF's implementation of Risk Management metric 10 was Ad Hoc (Level 1). USADF did not identify and define requirements for an automated solution to provide a centralized, enterprise wide (portfolio) view of cybersecurity risks across the organization, including risk control and remediation activities, dependences, risk scores/levels, and management dashboards, as required by the Defined maturity (Level 2) for metric 10.

Defined (Level 2) - USADF's implementation of Supply Chain Risk Management metric 14 was level 2.

Although USADF defined and communicated policies and procedures addressing cybersecurity and supply chain risk management requirements, USADF did not ensure that its policies, procedures, and processes were consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system or system component as required by the Consistently Implemented maturity (Level 3) for metric 14. Specifically, USADF relied on the contract in place for acquisition services for assessing supply chain risks. However, NIST requires that the review of supply-chain risks be performed by the organization receiving third-party services. Consequently, USADF's process of outsourcing the assessment of supply chain risk to the service provider did not meet NIST requirements.

Also, although USADF obtained sufficient assurance that the security controls of systems or services provided by contractors or other entities on behalf of the organization met FISMA requirements, OMB policy, and applicable NIST guidance, they did not obtain sufficient assurance of supply chain controls.

Furthermore, USADF did not maintain visibility into its upstream suppliers and cannot consistently track changes in suppliers.

Consistently Implemented (Level 3) – As discussed below, USADF consistently implemented Configuration Management metric 21, Identity and Access Management metric 32, and Contingency Planning metric 63. Therefore, its implementation of those three metrics was level 3.

- Configuration Management Metric 21 – USADF patched critical vulnerabilities within 30 days. However, via independent scans, CLA identified medium and low risk vulnerabilities due to missing patches and configuration weaknesses. Even though medium and low vulnerabilities were identified, CLA determined that these vulnerabilities are of lower risk to USADF. Further, CLA noted that, while USADF

managed its flaw remediation process, USADF did not utilize automated patch management and software update tools for operating systems as required by the Managed and Measurable maturity level (Level 4) for Metric 21. Additionally, USADF did not monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of flaw remediation processes which was also required by the Managed and Measurable maturity level for Metric 21.

- Identity and Access Management Metric 32 – Although USADF consistently implemented its processes for provisioning, managing, and reviewing privileged accounts across the agency and privileged user activities were logged and periodically reviewed, they did not employ automated mechanisms to support the management of privileged accounts as required by the Managed and Measurable maturity level (Level 4) for Metric 32.

- Contingency Planning Metric 63 – Although USADF consistently implemented system contingency plan testing and exercises, they did not employ automated mechanisms to test system contingency plans more thoroughly and effectively as required by the Managed and Measurable maturity level (Level 4) for Metric 63. In addition, USADF did not coordinate plan testing with external stakeholders (e.g., information and communications technology supply chain partners/providers), as appropriate which was also required by the Managed and Measurable maturity level for Metric 63.

2. USADF's Implementation of 15 of 20 FY 2022 Core Metrics was No Less Than Managed and Measurable

USADF's implementation of 4 metrics were Managed and Measurable (Level 4) and 11 metrics were Optimized (Level 5). The following paragraphs discuss each in detail.

Managed and Measurable (Level 4) - USADF's implementation was Managed and Measurable (level 4) for the following metrics: Configuration Management metric 20, Data Protection and Privacy metric 36, Incident Response metric 54, and Contingency Planning metric 61.

For example, USADF met the following Managed and Measurable requirements:

- Configuration Management Metric 20 - USADF employed automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to USADF's network and made appropriate modifications in accordance with organization-defined timelines. However, USADF did not deploy system configuration management tools that automatically enforce and redeploy configuration settings to systems required for the Optimized maturity level for metric 20.

- Incident Response Metric 54 - USADF monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures. In addition, USADF utilized profiling techniques to measure the characteristics of expected activities on its networks

and systems so that it could more effectively detect security incidents. Managed and Measurable is the highest maturity level for this metric.

- Contingency Planning Metric 61 - The results of USADF's Business Impact Analysis (BIA) were integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. In addition, USADF utilized the results of its BIA in conjunction with its risk register to inform senior level decision making. Managed and Measurable is the highest maturity level for this metric.

Optimized (Level 5) – USADF's implementation was Optimized (level 5) for the following metrics: Risk Management metrics 1-3, and 5; Identity and Access Management metrics 30 and 31; Data Protection and Privacy metric 37; Security Training metric 42; Information Security Continuous Monitoring metrics 47 and 49; and Incident Response metric 55.

For example, USADF met the following Optimized requirements:

- Risk Management Metric 1 - USADF used automation to develop and maintain a centralized information system inventory that included hardware and software components from all organizational information systems that was updated in a near-real time basis.

- Data Protection and Privacy Metric 37 - USADF's data exfiltration and enhanced network defenses were fully integrated into the ISCM and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications.

- Security Training Metric 42 - USADF's personnel collectively possessed a training level such that the USADF can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, USADF agreed with the evaluation results for the FY 2022 Core Metrics and provided a status of prior recommendations. USADF's comments are included in their entirety in Appendix II.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this evaluation was to determine the maturity level USADF achieved for each of its FY 2022 Core Metrics. For this evaluation, "Core metrics" are defined as the OMB Office of the Federal Chief Information Officer *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (FY 2022 Core Metrics). Therefore, this evaluation was not designed to determine causes of, effects of, or recommendations to improve the maturity levels.

Scope

We conducted this evaluation in accordance with *Quality Standards for Inspection and Evaluation*, issued by the Council of Inspectors General on Integrity and Efficiency.

For this year's review, IG's were required to assess 20 Core metrics in the following five security function areas to assess the maturity level and effectiveness of their agencies' information security program: Identify, Protect, Detect, Respond, and Recover. The maturity levels ranging from lowest to highest are Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

The scope of this evaluation was to assess USADF's information security program consistent with FISMA and reporting instructions issued by OMB and DHS. The scope also included assessing selected security controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of 3 of 11 internal and external information systems[9] in USADF's FISMA inventory as of February 16, 2022.

The evaluation also included follow up on prior audit recommendations from the fiscal year 2021 audit report[10] that tied to the FY 2022 Core Metrics to determine whether USADF made progress in implementing them. See Appendix IV for the status of the prior recommendations.

Evaluation fieldwork covered USADF's headquarters located in Washington, DC, from March 28, 2022, to July 7, 2022. It covered the period from October 1, 2021, through July 7, 2022.

Methodology

To assess USADF's information security program, we conducted interviews with USADF officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, we reviewed documents supporting the information security program.

[9] Ibid 5.
[10] Ibid 7.

These documents included, but were not limited to, USADF's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, we compared documents, such as USADF's information technology policies and procedures, to requirements stipulated in NIST special publications. We also performed tests of system processes to determine the adequacy of those controls. Finally, we reviewed the status of FISMA audit recommendations from fiscal year 2021.[11]

In assessing the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity (not the percentage of deficient items found compared to the total population available for review). In some cases, based on risk, significance, or criticality this resulted in selecting the entire population. However, in cases where the entire evaluation population was not selected, the results cannot be projected and if projected may be misleading.

To perform our evaluation of USADF's information security program and practices, we followed a work plan based on, but not limited to, the following guidance:

- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements.*
- OMB Office of the Federal Chief Information Officer *FY 2022 Core IG Metrics Implementation Analysis and Guidelines.*
- Council of the Inspectors General on Integrity and Efficiency (CIGIE), OMB, DHS, and the and the Federal Chief Information Officers and Chief Information Security Officers councils *FY 2022 Core IG FISMA Metrics Evaluation Guide*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource.*
- NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.
- NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.
- NIST Special Publication 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations.*
- NIST Special Publication 800-53B, Revision 5, *Control Baselines for Information Systems and Organizations.*
- CIGIE *Quality Standards for Inspection and Evaluation.*

[11] Ibid 7.

MANAGEMENT COMMENTS

Mr. Alvin Brown
Deputy Assistant Inspector General for Audit USAID,
Officer 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 FY 2022 (Report No. A-ADF-22-00X-C)

Dear Mr. Brown:
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.

Recommendation 1. (From FY21 FISMA Audit Finding)
We recommend that United States African Development Foundation'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.
We recommend that United States African Development Foundation'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.

Audit Status: Open

Evaluation results: Below core metrics of managed and measurable.

Management Response:
We accept the recommendation 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. Corrective action will be taken by March 31, 2023. The plan of action and milestones shall be updating for remediation and tracking.

Recommendation 2: This recommendation is closed. No further action is required.

Recommendation 3. (From FY21 FISMA Audit Finding)
We recommend that USADF's Chief Financial Officer design and implement a process to screen USADF contractors at the extent and level appropriate to the risks associated with the position.

Auditor's comment: Out of scope with regards to the FY22 Core metrics audited.

Management Response: We agree with auditor's comment.

Recommendation 4. (From FY21 FISMA Audit Finding)
We recommend that USADF's Chief Information Security Officer develop, document, and disseminate supply chain risk management procedures to facilitate the implementation of the USADF Supply Chain Risk Management Strategy & Policy.

Auditor's Comment: Out of scope with regards to the FY22 Core metrics audited.

Management Response: We agree with the auditor's comment.

Evaluation Results from the FY22 Core Metrics

- USADF's Implementation of 5 of 20 FY 2022 Core Metrics was Below Managed and Measurable
- USADF's Implementation of 15 of 20 FY 2022 Core Metrics was No Less Than Managed and Measurable

Management Response
USADF agrees with the evaluation results from the FY22 Core metrics.

SUMMARY OF RESULTS FOR EACH CORE METRIC

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
IDENTIFY					
Risk Management					
1. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections (NIST SP 800-53, Rev. 5: CA-3 and PM-5; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3; OMB A-130, NIST SP 800-37, Rev. 2: Task P-18; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5); CISA Cybersecurity & Incident Response Playbooks).					X
2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53, Rev. 5: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; NIST 800-207, 7.3.2; Federal Enterprise Architecture (FEA) Framework,					X

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
v2; FY 2022 CIO FISMA Metrics: 1.2-1.2.3; CSF: ID.AM-1, ID.AM-5; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 1).					
3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53, Rev. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2)?					X
5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels					X

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
(NIST SP 800-39; NIST SP 800-53, Rev. 5: RA-3 and PM-9; NIST IR 8286; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3)?					
10. To what extent does the organization utilize technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response)?	X				
IDENTIFY					
Supply Chain Risk Management					
14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements. (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5 and SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best		X			

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276, NIST 800-218, Task PO.1.3; FY 2022 CIO FISMA Metrics: 7.4.2; CIS Top 18 Security Controls v.8: Control 15).					
PROTECT					
Configuration Management					
20. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5; NIST SP 800-70, Rev. 4; FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing; EO 14028, Section 4, 6, and 7; OMB M-22-09, Federal Zero Trust Strategy, Section D; OMB M-22-05; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8, Controls 4 and 7; CSF: ID.RA-1 and DE.CM-8)?				X	
21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (EO 14028, Sections 3 and 4; NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; NIST 800-207, section 2.1; CIS Top 18 Security Controls v.8, Controls 4 and 7; FY 2022 CIO FISMA Metrics: Section 8; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02, 19-			X		

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
02, and 22-01; OMB M-22-09, Federal Zero Trust Strategy, Section D; CISA Cybersecurity Incident and Vulnerability Response Playbooks)?					
PROTECT					
Identity and Access Management					
30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; OMB M-19-17, NIST SP 800-157; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)?					X
31. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the					X

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17 and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; DHS ED 19-01; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)?					
32. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (EO 14028, Section 8; FY 2022 CIO FISMA Metrics: 3.1; OMB M-21-31; OMB M-19-17; NIST SP 800-53, Rev. 5: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4; CIS Top 18			X		

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
Security Controls v.8: Controls 5, 6, and 8).					
PROTECT					
Data Protection and Privacy					
36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle. (EO 14028, Section 3(d); OMB M-22-09, Federal Zero Trust Strategy; NIST 800-207; NIST SP 800-53, Rev. 5; SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6; CIS Top 18 Security Controls v. 8: Control 3)? • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse				X	
37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (FY 2022 CIO FISMA Metrics, 5.1; NIST SP 800-53, Rev. 5: SI-3, SI-7, SI-4, SC-7, and SC-18; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5, OMB M-21-07; CIS Top 18 Security Controls v.8: Controls 9 and 10)?					X

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
PROTECT					
Security Training					
42. To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (FY 2022 CIO FISMA Metrics, Section 6; NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS Top 18 Security Controls v.8: Control 14)?					X
DETECT					
Information Security Continuous Monitoring (ISCM)					
47. To what extent does the organization utilize ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31; NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6; CIS Top 18 Security Controls v.8: Control 13)?					X
49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and					X

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
maintaining system security plans, and monitoring system security controls (OMB A-130; NIST SP 800-137: Section 2.2; NIST SP 800-53, Rev. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03)					
RESPOND					
Incident Response					
54. How mature are the organization's processes for incident detection and analysis? (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17)				X	
55. How mature are the organization's processes for incident handling (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)					X

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
RECOVER					
Contingency Planning					
61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (FY 2022 CIO FISMA Metrics: 10.1.4; NIST SP 800-53, Rev. 5: CP-2, and RA-9; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; CSF:ID.RA-4)?				X	
63. To what extent does the organization perform tests/exercises of its information system contingency planning processes (FY 2022 CIO FISMA Metrics: 10.1; NIST SP 800-34; NIST SP 800-53, Rev. 5: CP-3 and CP-4; CSF: ID.SC-5 and CSF: PR.IP-10; CIS Top 18 Security Controls v.8: Control 11)?			X		
TOTAL	**1**	**1**	**3**	**4**	**11**

STATUS OF PRIOR YEAR RECOMMENDATIONS

The following table provides the status of the FY 2021[12] FISMA audit recommendations.

Report No.	No.	FY 2021 Audit Recommendation	USADF Position on Status	Auditor's Position on Status
No. A-ADF-22-001-C	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.	Closed	Open. See **Evaluation Results** **1. USADF's Implementation of 5 of 20 FY 2022 Core Metrics was Below Managed and Measurable**, Configuration Management
	2	We recommend that USADF's Chief Information Security Officer develop and implement a process to monitor privileged activities, including which activities to monitor as well as the process and frequency for monitoring those activities.	Closed	Closed. See **Evaluation Results** **1. USADF's Implementation of 5 of 20 FY 2022 Core Metrics was Below Managed and Measurable**, Identity and Access Management
	3	We recommend that USADF's Chief Financial Officer design and implement a process to screen USADF contractors at the extent and level appropriate to the risks associated with the position.	(Out of scope with regards to the FY 2022 Core Metrics and will be reviewed at a later time.)	
	4	We recommend that USADF's Chief Information Security Officer develop, document, and disseminate supply chain risk management procedures to facilitate the implementation of the USADF Supply Chain Risk Management Strategy & Policy.		

[12] Ibid 7.