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

USAID Implemented a Managed and Measurable Information Security Program for Fiscal Year 2022 in Support of FISMA

Report A-000-22-009-C
September 14, 2022

Information Technology Audits Division

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

MEMORANDUM

DATE: September 14, 2022

TO: USAID, Chief Information Officer, Jason Gray

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

SUBJECT: USAID Implemented a Managed and Measurable Information Security Program for Fiscal Year 2022 in Support of FISMA (A-000-22-009-C)

Enclosed is the final report on the evaluation of USAID'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 contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the evaluation. The contract required CLA 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 Quality Standards for Inspection and Evaluation, was not intended to enable us to express, and we do not express, an opinion on USAID's compliance with FISMA. CLA is responsible for the enclosed 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 USAID achieved for each of its core FISMA reporting metrics.[1] Therefore, it was not designed to determine causes of, effects of, or recommendations to improve the maturity levels.

To answer the objective, CLA evaluated the maturity level of USAID's implementation of the 20 core metrics. The scope of this evaluation was to assess whether USAID's information security program is consistent with FISMA reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security.[2] Also, CLA assessed selected security controls outlined in NIST Special Publication 800-53, Revision 5 *Security and Privacy Controls for Information Systems and Organizations* for a judgmental sample of 6 of 60 internal and external information systems in USAID's FISMA inventory as of February 11, 2022.

[1] For this evaluation, "core metrics" were defined as the fiscal year 2022 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."

Fieldwork covered USAID's headquarters located in Washington, DC. Fieldwork was performed from March 30, 2022, through July 7, 2022. It covered the period from October 1, 2021, through July 7, 2022.

CLA concluded that, for the 20 core metrics, USAID's information security program was optimized for 4 metrics, managed and measurable for 10 metrics, consistently implemented for 3 metrics, and defined for 3 metrics. Therefore, USAID's information security program was calculated as managed and measurable.

The report does not include recommendations. In response to our draft report, the Agency said it is committed to continuing to comply with FISMA requirements and safeguard USAID's Information Technology services to facilitate USAID's mission.

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

United States Agency for International Development Federal Information Security Modernization Act of 2014 Evaluation

Fiscal Year 2022

Final Report

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

phone 571-227-9500 **fax** 571-227-9552
CLAconnect.com

September 12, 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 Agency for International Development's (USAID) 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 USAID. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

S. M Mirzakhani

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
United States Agency for International Development

CliftonLarsonAllen LLP (CLA) conducted an evaluation of the United States Agency for International Development's (USAID) 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 USAID 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 USAID'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 6 of 60 internal and external systems in USAID's FISMA inventory of information systems.

Evaluation fieldwork covered USAID's headquarters located in Washington, DC, from March 30, 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, USAID's information security program was:

- Optimized for 4 metrics.
- Managed and Measurable for 10 metrics.
- Consistently Implemented for 3 metrics: and
- Defined for 3 metrics.

Therefore, USAID's information security program was calculated by CyberScope as Managed and Measurable.

In addition, we noted four recommendations from two prior FISMA audits remain open.

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 USAID on or before September 12, 2022. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 12, 2022.

The purpose of this evaluation report is to report on our evaluation of USAID'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 12, 2022

TABLE OF CONTENTS

Summary of Results....................1

Evaluation Results....................5

1. USAID's Implementation of 6 of 20 FY 2022 Core Metrics Was Below Managed and Measurable....................5

2. USAID's Implementation of 14 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....................12

Appendix IV – Status of Prior Year Recommendations....................22

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 USAID's information security program and practices. This evaluation was not designed to determine causes of, effects of, or recommendations to improve the maturity levels. Instead, the objective of this evaluation was to determine what maturity level USAID 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).

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 metrics, representing a combination of Administration priorities and other highly valuable controls, which 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 IG FISMA reporting 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
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 IG FISMA 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 6 of 60 internal and external information systems[5] in USAID's FISMA inventory as of February 11, 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, USAID's information security program was:

- Optimized for 4 metrics.
- Managed and measurable for 10 metrics.
- Consistently implemented for 3 metrics.
- Defined for 3 metrics.

Therefore, USAID's information security program was calculated by CyberScope as Managed and Measurable. 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	Defined	**Risk Management**	Defined
		Supply Chain Risk Management	Consistently Implemented
Protect	Managed and Measurable	**Configuration Management**	Optimized
		Identity and Access Management	Managed and Measurable
		Data Protection and Privacy	Managed and Measurable
		Security Training	Optimized
Detect	Managed and Measurable	**Information Security Continuous Monitoring (ISCM)**	Managed and Measurable
Respond	Optimized	**Incident Response**	Optimized
Recover	Managed and Measurable	**Contingency Planning**	Managed and Measurable
Overall	**Level 4: Managed and Measurable**		

[4] The controls were tested to the extent necessary to determine whether USAID implemented the processes specifically addressed in the FY 2022 Core Metrics. In addition, not all controls were tested for all six sampled information systems since several controls were inherited from the USAID 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.

In addition, we noted four recommendations from two prior FISMA audits[6] [7] remain open.

In response to the draft report, USAID acknowledged that the report contains no recommendations for action and that management is committed to continued improvements in managing its information security program. USAID's comments are included in their entirety in **Appendix II**.

The following section discusses the evaluation results in more detail related to USAID's implementation of each of the 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.

[6] Recommendations 2, 3, and 6 in *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2020 in Support of FISMA* (Audit Report No. A-000-21-004-C, January 7, 2021).

[7] Recommendation 2 in *USAID Implemented an Effective Information Security Program for Fiscal Year 2021 in Support of FISMA* (Audit Report No. A-000-22-005-C, December 7, 2021).

EVALUATION RESULTS

1. USAID’s Implementation of 6 of 20 FY 2022 Core Metrics was Below Managed and Measurable

USAID’s implementation of metrics 2, 3, 10, 14, 37, and 63 was below Managed and Measurable (Level 4). The following paragraphs discuss each in detail.

Defined (Level 2) - USAID’s implementation of Risk Management metrics 2, 3, and 10 was Defined (Level 2). Specifically, for Risk Management:

- Metric 2, USAID defined its policies, procedures, and processes for using standard data elements to develop and maintain an up-to-date inventory of hardware assets that are connected to the agency’s network. However, USAID did not consistently maintain an up-to-date inventory of hardware assets, as required by the Consistently Implemented (Level 3) maturity level for metric 2. Specifically, the serial number was not documented for 537 hardware assets out of 85,230 total assets. In addition, there were 1,228 duplicate serial numbers out of 85,230 total assets. Furthermore, in a revised inventory,[8] the specific location or owner of 2,047 deployed assets was not documented out of 84,809 total assets; 1,300 of these assets were servers, laptops, and networking equipment.

- Metric 3, USAID defined its policies, procedures, and processes for using standard data elements to develop and maintain an up-to-date inventory of software assets and licenses utilized in the agency’s environment. However, USAID did not consistently maintain an up-to-date inventory of software assets and licenses, as required by the Consistently Implemented (Level 3) maturity level for metric 3. Specifically, 23 out the total population of 115 (20%) entries in the software license inventory were missing the license quantity information. Upon notification of this issue to management, the license quantities were added for those software items.

- Metric 10, USAID defined requirements for an automated solution to provide a centralized, enterprise-wide view of cybersecurity risks across the agency. However, the automated solution was not fully implemented, as required by the Consistently Implemented (Level 3) maturity level for metric 10.

Consistently Implemented (Level 3) – As discussed below, USAID consistently implemented Supply Chain Risk Management metric 14, Data Protection and Privacy metric 37, and Contingency Planning metric 63. Therefore, its implementation of those three metrics was level 3.

- Supply Chain Risk Management (Metric 14) – USAID ensured 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, system component. In addition, USAID incorporated supplier risk

[8] Upon notification of the duplicate serial numbers in the inventory, management removed the duplicates and provided a revised inventory for review.

evaluations into its continuous monitoring practices to maintain situational awareness into the supply chain risks. However, USAID did not use qualitative and quantitative performance metrics to measure, report on, and monitor the information security and supply chain risk management performance of products, systems, and services provided by external providers, as required by the Managed and Measurable (Level 4) maturity level for Metric 14.

- Data Protection and Privacy (Metric 37) – USAID consistently monitored inbound and outbound network traffic, ensuring that all traffic passed through a web content filter that protected against phishing, malware, and blocked against known malicious sites. In addition, USAID utilized email authentication technology and ensured the use of valid encryption certificates for its domains. However, USAID did not monitor its Domain Name System (DNS) infrastructure for potential tampering or audit its DNS records, as required by the Managed and Measurable (Level 4) maturity level for Metric 37.

- Contingency Planning (Metric 63) – USAID consistently tested information system contingency plans and integrated testing to the extent practicable with related plans, such as the incident response plan and continuity of operations plan. However, USAID did not employ automated mechanisms to test system contingency plans more thoroughly and effectively, as required by the Managed and Measurable (Level 4) maturity level for Metric 63. In addition, USAID 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. USAID's Implementation of 14 of 20 FY 2022 Core Metrics was No Less Than Managed and Measurable

USAID's implementation of 10 metrics was Managed and Measurable (Level 4) and 4 metrics was Optimized (Level 5). The following paragraphs discuss each in detail.

Managed and Measurable (Level 4) - USAID's implementation was Managed and Measurable (Level 4) for the following metrics: Risk Management metric 1; Configuration Management metric 20; Identity and Access Management metrics 30-32; Data Protection and Privacy metric 36; ISCM metrics 47 and 49; Incident Response metric 54; and Contingency Planning metric 61.

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

- Risk Management (Metric 1) – The information systems included in USAID's inventory were subject to the monitoring process defined within the agency's ISCM strategy. However, USAID did not use automation to develop and maintain a centralized information system inventory that included hardware and software components from all organizational information systems required for the Optimized maturity level for Metric 1.

- Data Protection and Privacy (Metric 36) – USAID monitored security controls for protecting personally identifiable information and other agency sensitive data, as appropriate, throughout the data lifecycle as defined within the agency's ISCM strategy. However, USAID did not implement the following enhanced protective capabilities: dual authorization for sanitization of media devices; exemption of media marking as long as the media remains within USAID specified controlled areas; and configuring systems to record the date the personally identifiable information was collected, created, updated or deleted/destroyed required for the Optimized maturity level for Metric 36.

- Incident Response (Metric 54) – USAID monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures. Additionally, USAID 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 USAID's Business Impact Analysis (BIA) was integrated with enterprise risk management processes for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. In addition, USAID 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) - USAID's implementation was Optimized (level 5) for the following metrics: Risk Management metric 5, Configuration Management metric 21, Security Training metric 42, and Incident Response metric 55. Specifically, USAID met the following Optimized requirements:

- Risk Management (Metric 5) - USAID fully integrated cybersecurity risk management at the organizational, mission/business process, and information system levels. Additionally, USAID utilized Cybersecurity Framework profiles to align cybersecurity outcomes with mission or business requirements, risk tolerance, and resources of the organization.

- Configuration Management (Metric 21) – USAID employed automated patch management and software update tools for applications and network devices (including mobile devices) as appropriate, where such tools are available and safe.

- Security Training (Metric 42) – USAID's personnel collectively possessed a training level such that the agency demonstrated that security incidents resulting from personnel actions or inactions were being reduced over time.

- Incident Response (Metric 55) – USAID utilized dynamic reconfiguration (e.g., changes to router rules, access controls list, and filter rules for firewalls and gateways) to manage attacks, misdirect attackers, and to isolate components of systems.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, USAID acknowledged that the report contains no recommendations for action and that management is committed to continued improvements in managing its information security program. USAID'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 USAID 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). Given the objective, 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 the *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency.

For this year’s review, IGs 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 USAID’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 Information Systems and Organizations*, for a sample of 6 of 60 internal and external information systems[9] in USAID’s FISMA inventory as of February 11, 2022.

The evaluation also included follow up on FISMA audit recommendations from fiscal years 2020[10] and 2021[11] that tied to the FY 2022 Core Metrics to determine whether USAID made progress in implementing them. See Appendix IV for the status of the prior recommendations.

Evaluation fieldwork covered USAID’s headquarters located in Washington, DC., from March 30, 2022, to July 7, 2022. It covered the period from October 1, 2021, through July 7, 2022.

[9] Ibid 5.

[10] Ibid 6.

[11] Ibid 7.

Methodology

To assess USAID's information security program, we conducted interviews with USAID officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, we reviewed documents supporting the information security program. These documents included, but were not limited to, USAID'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 USAID's information technology policies and procedures, to requirements stipulated in NIST special publications. We also performed tests of system processes to determine the adequacy and effectiveness of those controls. Finally, we reviewed the status of FISMA audit recommendations from fiscal years 2020,[12] and 2021.[13]

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 population was not selected, the results cannot be projected and if projected may be misleading.

To perform our evaluation of USAID'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 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, Revisions 5, *Control Baselines for Information Systems and Organizations.*
- CIGIE *Quality Standards for Inspection and Evaluation.*

[12] Ibid 6.
[13] Ibid 7.

MANAGEMENT COMMENTS

USAID
FROM THE AMERICAN PEOPLE

MEMORANDUM

TO: **Deputy Assistant Inspector General for Audit, Alvin A. Brown**

FROM: **USAID Chief Information Officer, Jason Gray M/CIO** /S/

DATE: August 24, 2022

SUBJECT: Management Comment(s) to Respond to the Draft Evaluation Report Produced by the Office of Inspector General (OIG) titled, *USAID's Information Security Program for Fiscal Year 2022 in Support of FISMA was Calculated as Managed and Measurable*

The U.S. Agency for International Development (USAID) would like to thank the Office of Inspector General (OIG) for the opportunity to provide comments on the subject draft report. The Agency noted that the report contains no recommendations for action. USAID is committed to supporting improvements to managing our information security program as required by the Federal Information Security Modernization Act of 2014 (FISMA). The OIG acknowledges this commitment in the draft report, by recognizing that our agency had an effective agency-wide information security program in Fiscal Year 2022.

In compliance with FISMA, USAID has developed, documented, and implemented an agency-wide program to provide information security for the information and information systems (ISs) that support the operations and assets of the agency. USAID is committed to continuing to comply with FISMA requirements and safeguard USAID's Information Technology services to facilitate USAID's mission.

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		X			

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
8011; NIST 800-207, 7.3.2; Federal Enterprise Architecture (FEA) Framework, 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					X

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
information system security risks are adequately managed at the organizational, mission/business process, and information system levels (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			X		

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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 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;					X

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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, 19-02, 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;				X	

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)?					
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 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)?				X	
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				X	

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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 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	

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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		
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				X	

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
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)?					
49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and 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)				X	
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,				X	

Metric	Assessed Maturity Level				
	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17)					
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
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	**0**	**3**	**3**	**10**	**4**

STATUS OF PRIOR YEAR RECOMMENDATIONS

The following tables provide the status of the FY 2020, and FY 2021[14] FISMA audit recommendations.

Report No.	No.	FY 2020 Audit Recommendation	USAID Position on Status	Evaluator's Position on Status
A-000-21-004-C	2	We recommend USAID's Chief Information Officer should collaborate with the Office of Human Capital and Talent Management to document and implement a process to verify that separated employees' accounts are disabled in a timely manner in accordance with Agency policy.	Open	Agree based on review of management's target completion date of July 1, 2022.[15]
A-000-21-004-C	3	We recommend USAID's Office of Human Capital and Talent Management should implement a process to maintain records electronically for onboarding and off-boarding staff.	Open	Agree based on review of management's target completion date of July 1, 2022.[16]
A-000-21-004-C	6	We recommend USAID's Chief Information Officer develop and implement a process to block unauthorized applications from installing on Agency mobile devices.	Open	Agree based on review of management's target completion date of September 30, 2022.

Report No.	No.	FY 2021 Audit Recommendation	USAID Position on Status	Evaluator's Position on Status
A-000-22-005-C	2	We recommend USAID's Chief Information Officer should address the management of system components requiring repair or service in its Supply Chain Risk Management Standard Operating Procedures.	Open	Agree based on review of management's target completion date of September 30, 2022.

[14] Ibid 6 and 7.

[15] In order to meet our contractual requirement of June 10, 2022 for the draft FISMA reporting metrics, the cutoff date for USAID to provide evidence for closure of prior year recommendations that were tied to the FY 2022 Core Metrics was May 13, 2022.

[16] Ibid 15.