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

USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA

AUDIT REPORT A-000-20-005-C
FEBRUARY 7, 2020

1300 Pennsylvania Avenue NW • Washington, DC 20523
https://oig.usaid.gov • 202-712-1150

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under OIG's jurisdiction: the U.S. Agency for International Development, Millennium Challenge Corporation, U.S. African Development Foundation, Inter-American Foundation, and Overseas Private Investment Corporation.

Report waste, fraud, and abuse

USAID OIG Hotline
Email: ig.hotline@usaid.gov
Complaint form: https://oig.usaid.gov/complainant-select
Phone: 202-712-1023 or 800-230-6539
Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657

MEMORANDUM

DATE: February 7, 2020

TO: USAID, Deputy Assistant Administrator, AA/M, Albert G. Bullock
USAID, M/CIO, Chief Information Officer, Jay Mahanand

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

SUBJECT: USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA (A-000-20-005-C)

Enclosed is the final audit report on USAID's information security program for fiscal year 2019 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 Clifton Larson Allen (CLA), LLC, to conduct the audit. The contract required CLA to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed CLA's report and related audit documentation and inquired of its representatives. Our review, which was different from an audit performed in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on USAID's compliance with FISMA. CLA is responsible for the enclosed auditor's 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 audit objective was to determine whether USAID implemented an effective information security program.[1] To answer the audit objective, CLA tested USAID's implementation of selected controls outlined in the National Institute of Standards and Technology's Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." CLA reviewed 6 of 45 information systems in USAID's systems inventory as of May 21, 2019. Fieldwork took place at USAID's headquarters in Washington, DC, from May 13 to October 24, 2019. It covered the period from October 1, 2018, through September 30, 2019.

[1] For this audit, an effective information security program was defined as implementing certain security controls for selected information systems in support of FISMA.

The audit firm concluded that USAID generally implemented an effective information security program by implementing 144 of 157 instances of selected security controls for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of the Agency's information and information systems. Among those controls, USAID maintained an effective:

- Information system continuous monitoring strategy.
- Security training program.
- Incident handling and response program.

The audit firm also identified weaknesses. For example, as summarized in the table below, CLA noted weaknesses in five of the eight FISMA metric domains. With these weaknesses, USAID's information and information systems are potentially exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

Fiscal Year 2019 IG FISMA Metric Domains[2]	**Weaknesses Identified**
Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	X
Security Training	
Information Security Continuous Monitoring	
Incident Response	
Contingency Planning	X

To address the weaknesses identified in CLA's report, we are recommending the following actions.

Recommendation 1. USAID's chief information officer should document and implement a process to confirm that approval of user access is documented prior to granting access to the system for which verbal approvals had been allowed.

Recommendation 2. USAID's chief information officer should update its hardware inventory policies to reflect the current operating environment.

Recommendation 3. USAID's senior Agency official for privacy should document and implement a process to continuously monitor and review privacy controls in accordance with the Privacy Continuous Monitoring Strategy.

[2] Office of Management and Budget, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency's "FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," April 9, 2019.

Recommendation 4. USAID's chief information officer should update the system security plan to document the frequency with which position risk designations are to be reviewed and updated.

Recommendation 5. USAID's chief information officer should document backup procedures for the current operating environment.

Recommendation 6. USAID's chief information officer should update acquisition policies and procedures to include security requirements outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, control SA 4 – Acquisition Process, for all information technology acquisitions.

Recommendation 7. USAID's chief information officer should conduct a documented review of National Institute of Standards and Technology Special Publication 800-160, Volume 1, to identify security engineering principles that are applicable to the Agency and update the Agency's "SDLC Process Description Document" accordingly.

In finalizing the report, CLA evaluated USAID's responses to the recommendations. After reviewing that evaluation, we consider recommendations 1 and 5 resolved but open pending OIG's verification of the Agency's final actions and recommendations 2 and 3 resolved but open pending completion of planned activities. We consider recommendations 4 and 7 closed upon issuance of this report. We consider recommendation 6 open and unresolved because of the audit firm's disagreement with the Agency's closure request.

For recommendations 2 and 3, please provide evidence of final action to the Audit Performance and Compliance Division. Please work with us to resolve recommendation 6.

We appreciate the assistance extended to our staff and CLA employees during the engagement.

United States Agency for International Development

Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2019

Final Report

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

January 24, 2020

Mr. Mark Norman
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 Mr. Norman:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the results of our audit 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) of fiscal year 2019.

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

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
United States Agency for International Development

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the United States Agency for International Development's (USAID) information security program and practices for fiscal year 2019 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether USAID implemented an effective information security program. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls from 6 of USAID's 45 information systems. Audit fieldwork was performed at USAID's headquarters in Washington, DC, and Arlington, VA, from May 13, 2019 to October 24, 2019.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We concluded that USAID generally implemented an effective information security program by implementing many of the selected security controls for selected information systems. Although USAID generally implemented an effective information security program, its implementation of a subset of selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, we noted weaknesses in 5 of the 8 Inspector General FISMA Metric Domains and have made 7 recommendations to assist USAID in strengthening its information security program.

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 performance audit to future periods is subject to the risks that conditions may materially change from their current status. We concluded our fieldwork and assessment on October 24, 2019. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 24, 2019.

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

Additional information on our findings and recommendations are included in the accompanying report. We are submitting this report to USAID Office of Inspector General.

CliftonLarsonAllen LLP

Arlington, Virginia
January 24, 2020

TABLE OF CONTENTS

SUMMARY OF RESULTS

Background

The United States Agency for International Development's (USAID) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an annual evaluation of USAID's information security program and practices. The objective of this performance audit was to determine whether USAID implemented an effective[2] information security program.

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. All agencies must also report annually to the Office of Management and Budget (OMB) and to congressional committees on the effectiveness of their information security program.

FISMA also requires Agency Inspectors General (IGs) to assess the effectiveness of Agency information security programs and practices. OMB and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards to establish Agency baseline security requirements.

OMB and the Department of Homeland Security (DHS) annually provide instructions to federal agencies and IGs for preparing FISMA reports. On October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 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[3] to independently assess their agencies' information security programs.

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

[2] For this audit, an effective information security program is defined as implementing certain security controls for selected information systems in support of FISMA.

[3] CLA submitted its responses to the FY 2019 IG FISMA Reporting Metrics to USAID OIG as a separate deliverable under the contract for this performance audit.

The fiscal year (FY) 2019 IG FISMA Reporting Metrics are designed to assess the maturity[4] of the information security program and align with the 5 functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.3: Identify, Protect, Detect, Respond, and Recover, as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains
Identify	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

For this audit, CLA reviewed selected[5] controls related to the IG FISMA Reporting Metrics from 6 of 45 information systems[6] in USAID's FISMA inventory as of May 21, 2019.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. CLA believes that the evidence obtained provides a reasonable basis for CLA's findings and conclusions based on the audit objective.

Audit Results

CLA concluded that USAID generally implemented an effective information security program by implementing 144 of 157 instances of the selected security controls for selected information systems. For example, USAID maintained an effective:

- Information system continuous monitoring strategy.
- Security training program.
- Incident handling and response program.

Although USAID generally implemented an effective information security program, its implementation of 13 of the 157 control instances was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption,

[4] The five levels in the maturity model are: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized. To be considered effective, an agency's information security program must be rated at least Managed and Measurable (Level 4).
[5] See Appendix III for a list of controls selected.
[6] 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.

modification, or destruction. As a result, CLA noted weaknesses in 5 of the 8 FISMA Metric Domains (Table 2) and made 7 recommendations to assist USAID in strengthening its information security program.

Table 2: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2019 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains	Weaknesses Noted in FY 2019
Identify	**Risk Management**	USAID Needs to Strengthen Vulnerability and Patch Management Controls (**Finding 1**) USAID Needs to Strengthen System and Service Acquisition Controls (**Finding 7**)
Protect	**Configuration Management**	USAID Needs to Strengthen Configuration Management Controls (**Finding 3**)
	Identity and Access Management	USAID Needs to Strengthen Account Management Controls (**Finding 2**) USAID Needs to Update Personnel Security Controls (**Finding 5**)
	Data Protection and Privacy	USAID Needs to Conduct a Continuous Review of Privacy Controls (**Finding 4**)
	Security Training	No weaknesses noted.
Detect	**Information Security Continuous Monitoring**	No weaknesses noted.
Respond	**Incident Response**	No weaknesses noted.
Recover	**Contingency Planning**	USAID Needs to Update Back-up Policies and Procedures (**Finding 6**)

In response to the draft audit report, USAID outlined its plans to address all 7 recommendations. We acknowledge USAID's management decisions on recommendations 1 through 5 and 7. Based on our evaluation of the Agency's comments, we do not agree with closure for recommendation 1 because there has not been sufficient time to determine if the corrective actions have been fully implemented. Therefore, we consider recommendation 1 resolved, but open pending OIG's verification of the Agency's final actions. We consider recommendations 2 and 3 resolved but open pending completion of planned activities. We consider recommendation 4 closed upon issuance of this report. We do not agree that recommendation 5 should be closed because USAID needs to provide additional support to demonstrate that the updated documentation reflects the current operating environment. Therefore, we consider recommendation 5 resolved but open pending OIG's verification of the Agency's final actions. We consider recommendation 6 open-unresolved because we do not agree that the actions taken by management were sufficient to close the recommendation. We

consider recommendation 7 closed upon issuance of this report. USAID's comments are included in their entirety in Appendix II without the supporting documents.

The following section provides a detailed discussion of the audit findings. Appendix I describes the audit scope and methodology.

AUDIT FINDINGS

1. USAID Needs to Strengthen Vulnerability and Patch Management Controls

Cybersecurity Framework Security Function: *Identify*
FY 19 FISMA IG Metric Domain: *Risk Management*

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* security control SI-2, states the following regarding patch management:

> The organization:
> * * *
> c. Installs security-relevant software and firmware updates within [*Assignment: organization defined time period*] of the release of the updates.

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, states:

> i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems.
>
> Agencies shall:
> * * *
> 8. Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement; and
> 9. Implement and maintain current updates and patches for all software and firmware components of information systems.

Additionally, USAID's *Unauthorized/Unsupported Software Standard Operating Procedure* states that the Operations and Maintenance Desktop Team will "either upgrade or remove the unsupported software within 48 hours."

USAID's internal monthly vulnerability scans[7] of its network identified critical security vulnerabilities related to patch management and unsupported software. Although some of the vulnerabilities were within the allowable timeframe for them to be remediated, others were past the required remediation timeframe. Management indicated they were aware of the vulnerabilities and taking steps to remediate them; however, USAID encountered challenges in obtaining an updated software license needed to remediate the identified vulnerabilities.

[7] USAID performed the vulnerability scans during June 2019.

Unmitigated vulnerabilities on USAID's network can compromise the confidentiality, integrity, and availability of information on the network. For example:

- An attacker may leverage known vulnerabilities to execute arbitrary code.
- Authorized USAID employees may be unable to access systems.
- USAID data may be lost, stolen, or compromised.

Furthermore, unsupported systems may be susceptible to older vulnerabilities and exploits that vendors have addressed with current supported versions. OIG made two recommendations to address this weakness in its FY 2018 FISMA audit report.[8] Therefore, we are not making additional recommendations at this time.

2. USAID Needs to Strengthen Account Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Identity and Access Management*

NIST SP 800-53, Revision 4, security control AC-2, states the following regarding account management:

> The organization:
> * * *
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].

In addition, the USAID *Information System Security Officer (ISSO) Handbook* states the following regarding access authorizations:

> The ISSO, in collaboration with the System Owner [SO] or other designees, should:
> * * *
> C. Ensure signed (paper or electronic) or approved access request documentation is maintained for each user account.

Controls were not adequate to ensure USAID performed effective account management for 1 of 6 sampled systems tested. Specifically, from a sample of 17 user access requests from the total population of 166 new users, 2 user access requests could not be provided.

According to system managers, the 2 user access requests could not be provided because the request were made verbally, which they said was an approved method for granting access. However, CIO officials said that verbal access was not allowed.

If user access is not approved and documented in accordance with policy, users may be given inappropriate access to sensitive data that is not needed to perform their duties. Therefore, CLA is making the following recommendation.

[8] Recommendations 1 and 2 in *USAID Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-19-005-C, November 21, 2018).

Recommendation 1: *USAID's Chief Information Officer document and implement a process to confirm that approval of user access is documented prior to granting access to the system for which verbal approvals had been allowed.*

3. USAID Needs to Strengthen Configuration Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Configuration Management*

USAID Automated Directives System (ADS) Chapter 545, Section 545.3.6.3, states, "System Owners must test, validate, and document changes to the information system before implementing the changes on the operational system." It further states in Section 545.3.6.4 that the Chief Information Officer:

> …must analyze proposed changes to the information system to determine potential security impacts prior to change implementation, and make recommendations based on that analysis.

USAID ADS Chapter 545, Section 545.3.6.8, states:

> System Owners must:
> …
> d. Ensure the inventory is at the level of granularity deemed necessary for tracking and reporting. The inventory specifications include:
> 1. Vendor/manufacture name and component name;
> 2. Hardware model number, item description, and serial number;
> 3. Hardware configuration;
> 4. Software version number and description;
> 5. Software license information including seats, number of licenses, etc. as applicable; and
> 6. Physical location of hardware.

USAID did not follow its system change and inventory management procedures as follows:

- USAID did not perform testing, risk analysis and approval for 3 of 6 systems tested:
  - For one system, 7 of the 25 sampled change requests, from a total population of 797 change requests, did not have test results documented and 3 of 25 change requests did not have test plans documented.
  - All 15 sampled change requests for a second system, from a total population of 150 change requests, did not have evidence that security impact analyses were performed.
  - For 1 of 2 sampled change requests, from a total population of 13 change requests for a third system, the following evidence was not provided:
    - Change Control Board Approval
    - Security Impact Analysis
    - Test Plan

        - Test Plan Results
        - Approval to Implement

- USAID did not include the following fields in the hardware inventory as required by USAID ADS Chapter 545 Section 545.3.6.8:
    - Vendor/manufacture name
    - Hardware Configuration
    - Software Version Number and description

Management stated that not all required change documentation was maintained because 2 of the 3 systems had not yet incorporated the new change management procedures established in the *Application Operation and Maintenance (APP O&M) Configuration Management Plan (CMP)* issued January 16, 2019. In addition, one system did not have all required information captured because proper reviews of the change requests were not completed before it was approved for implementation. Management stated the inventory issue occurred because the requirements in ADS Chapter 545 were outdated and no longer reflective of the information that management intends to collect and is currently collecting.

Without following proper change management procedures, including assessments of risk and testing of system changes, security deficiencies and vulnerabilities may exist and go undetected. In addition, system changes may not operate as intended causing functionality issues for end users.

Additionally, without a proper hardware inventory listing, incomplete or inaccurate inventories could result in a loss of confidentiality and waste. Stolen or misplaced computing equipment could put USAID at a risk of loss of control of their data, including personally identifiable information. This may also cause a strain on the USAID budget as unplanned and unnecessary spending may be required to replace stolen or misplaced computing equipment. OIG made a recommendation to address the testing, assessing risk and approving configuration changes in its FY 2018 FISMA audit report.[9] Therefore, we are not making additional recommendations at this time. However, CLA is making one new recommendation regarding hardware inventories.

Recommendation 2: *USAID's Chief Information Officer should update its hardware inventory policies to reflect the current operating environment.*

[9] Recommendation 5, *USAID Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-19-005-C, November 21, 2018).

4. USAID Needs to Conduct a Continuous Review of Privacy Controls

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Data Protection and Privacy*

NIST SP 800-53, Revision 4, privacy control AR-4, states the following regarding privacy monitoring and auditing, "the organization monitors and audits privacy controls and internal privacy policy [*Assignment: organization-defined frequency*] to ensure effective implementation."

USAID has not continuously monitored and performed reviews of privacy controls as required by USAID's *Privacy Continuous Monitoring Strategy*. Agency management had not developed the control assessment schedule and method contained in its *Privacy Continuous Monitoring Strategy*. According to Agency management, there was insufficient staff to complete the assessment strategy and to perform monitoring and auditing of the privacy controls.

Without continuously monitoring privacy controls, USAID may not be able to determine the extent to which the controls are operating effectively or as intended. Moreover, USAID may not be able to determine whether controls are sufficient to ensure compliance with applicable privacy requirements. Therefore, CLA is making the following recommendation.

> ***Recommendation 3:*** *USAID's Senior Agency Official for Privacy should document and implement a process to continuously monitor and review privacy controls in accordance with the* Privacy Continuous Monitoring Strategy*.*

5. USAID Needs to Update Personnel Security Controls

Cybersecurity Framework Security Function: *Protect*
FY 19 FISMA IG Metric Domain: *Identity and Access Management*

The system security plan, security control PS-2, states the following regarding position risk designation:

> The organization:
> * * *
> c. Reviews and updates position risk designations annually.

USAID was not reviewing position risk designations on an annual basis as noted in the system security plan. Instead, Agency management said that they review position risk designations every 3 to 5 years. Agency management stated there was an error made when entering this parameter in the Cyber Security Assessment and Management system, which caused the wrong review cycle to be noted within the system security plan.

Without proper control frequencies documented, USAID cannot ensure position risk designations are reviewed and updated appropriately. Therefore, CLA is making the following recommendation.

> ***Recommendation 4:*** *USAID's Chief Information Officer should update the* system security plan *to document the frequency with which position risk designations are to be reviewed and updated.*

6. USAID Needs to Update Back-up Policies and Procedures

Cybersecurity Framework Security Function: *Recover*
FY 19 FISMA IG Metric Domain: *Contingency Planning*

NIST SP 800-53, Revision 4, security control CP-1, states the following regarding contingency planning policies and procedures:

> The organization:
> a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
> ***
> 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

ADS Chapter 545, Section 545.3.7.1, states:

> The Chief Information Security Officer (CISO) must develop, document, review annually, update as required, and disseminate to the USAID staff a contingency planning policy. SOs must document, implement, and enforce procedures to comply with contingency planning policies and associated contingency plan control requirements.

USAID's backup policy and procedures are outdated and do not reflect the current operating environment. Specifically, the policy and procedures referenced an old location for backup tapes that is no longer used and an outdated backup methodology. Management indicated that the backup policy and procedures are outdated due to the transition of the system to Amazon Web Services. Management stated there is an updated backup architecture, which shows how backups are being performed; however, it was not provided during the assessment period.

Without updated backup policy and procedures, backups may not be properly performed and Agency data is at risk of being lost. Therefore, CLA is making the following recommendation.

> ***Recommendation 5:*** *USAID's Chief Information Officer should document backup procedures for the current operating environment.*

7. USAID Needs to Strengthen System and Services Acquisition Controls

Cybersecurity Framework Security Function: *Identify*
FY 19 FISMA IG Metric Domain: *Risk Management*

NIST SP 800-53, Revision 4, security control SA-4, states the following regarding acquisition process:

> Control Enhancement 9: The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.
>
> Control Enhancement 10: The organization employs only information technology products on the [Federal Information Processing Standards] (FIPS) 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems

NIST SP 800-53, Revision 4, security control SA-9, states the following regarding external information system services:

> The organization:
> a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
>
> Control Enhancement 2: The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services.

NIST SP 800-53, Revision 4, security control SA-8, security engineering principles, states, "the organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system."

USAID policies and procedures did not address the following system and services acquisition requirements:

- How developers of information systems/services are required to document functions, ports, protocols, or services early on in the development process;
- The use of FIPS 201-approved products; and
- How USAID will ensure that security controls of systems or services provided by contractors or other entities on behalf of the organization will meet FISMA requirements, OMB policy, and applicable NIST guidance.

Management stated that the information was not included because they believe these items were inherent to the acquisition process. Management also stated there is an approved listing of ports, protocols, and services that are allowed to be used within the USAID infrastructure. However, this document did not require functions, ports, protocols, or services to be identified and documented.

Additionally, USAID's *System Development Life Cycle (SDLC)-Agile Process Description Document* did not include system security engineering principles documented in NIST SP 800-160, Volume 1, *Systems Security Engineering*. Some examples include:

- Assessing the security aspects of the management and technical plans against objectives to determine adequacy and feasibility.
- Confirming that the delivered product or service complies with the security aspects of the agreement.
- Defining and recording the security risk thresholds and conditions under which a level of risk may be accepted.

Management stated they believed NIST SP 800-160 was guidance and not required and therefore did not document how security engineering principles are incorporated into the system development life cycle.

Without proper documentation of acquisition requirements and security engineering documentation, USAID runs the risk of acquiring hardware and software without having proper security measures in place. This presents the opportunity for USAID to acquire non-compliant solutions increasing the risk of data breaches and/or vulnerabilities. Therefore, CLA is making the following recommendations.

> ***Recommendation 6:*** *USAID's Chief Information Officer should update acquisition policies and procedures to include security requirements outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, control SA 4 – Acquisition Process, for all information technology acquisitions.*
>
> ***Recommendation 7:*** *USAID's Chief Information Officer should conduct a documented review of National Institute of Standards and Technology Special Publication 800-160, Volume 1, to identify security engineering principles that are applicable to the Agency and update the Agency's* SDLC Process Description Document *accordingly.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, USAID outlined its plans to address all 7 recommendations. USAID's comments are included in their entirety in Appendix II. Based on our review of management's comments, we acknowledge management decisions on recommendations 1 through 5 and 7. However, we do not acknowledge the management decision for recommendation 6.

For recommendations 2 and 3, USAID provided its proposed corrective action plans to address the weaknesses. Therefore, we consider these recommendations resolved but open pending completion of planned activities.

For recommendations 1, 4, 5, 6, and 7, USAID requested closure upon issuance of the final report. Below is our evaluation of management's request for closure:

For recommendation 1, we agree the *Account Management Procedures* have been updated to address user access approval. However, there has not been sufficient time to determine if management has implemented a process to confirm that approval of user access is documented prior to granting access to the system. Therefore, we consider recommendation 1 resolved but open pending OIG's verification of the Agency's final actions.

For recommendation 4, we agree the system security plan has been updated to document the frequency with which position risk designations are to be reviewed and updated. Therefore, we consider recommendation 4 closed upon issuance of this report.

For recommendation 5, while updated backup procedures have been documented, we are unable to validate their accuracy without additional documentation to ensure the updated backup procedures reflect the current operating environment. Therefore, we do not agree recommendation 5 should be closed yet. We consider recommendation 5, resolved but open pending OIG's verification of the Agency's final actions.

For recommendation 6, while updates were made to the acquisition policies and procedures, they were still missing requirements from NIST SP 800-53 Revision 4 security control SA-4. Specifically, there was no requirement for the system developer to define the functions, ports, protocols, and services the new system will use. Therefore, we do not agree that recommendation 6 should be closed. We consider recommendation 6 open-unresolved because the corrective actions taken for final action were not sufficiently responsive to the recommendation.

For recommendation 7, we agree a documented review of NIST SP 800-160, Volume 1, has been performed and applicable security engineering principles have been identified. Therefore, we consider recommendation 7 closed upon issuance of this report.

SCOPE AND METHODOLOGY

Scope

CLA conducted this audit in accordance with GAGAS. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit was designed to determine whether USAID implemented an effective[10] information security program.

The audit included tests of selected management, technical, and operational controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. CLA assessed USAID's performance and compliance with FISMA in the following areas:

- Access Controls
- Accountability, Audit, and Risk Management
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Media Protection
- Personnel Security
- Planning
- Program Management
- Risk Assessment
- Security
- Security Assessment and Authorization
- System and Communications Protection
- System and Information Integrity
- System and Service Acquisition

For this audit, CLA reviewed selected controls related to the FY 2019 IG FISMA Reporting Metrics from 6 of 45 judgmentally selected information systems in USAID's systems inventory as of May 21, 2019.[11] See Appendix III for a listing of the 157 control instances we tested.[12]

[10] For this audit, an effective information security program is defined as implementing certain security controls for selected information systems in support of FISMA.

[11] The systems were selected based on risk to the Agency.

[12] There were 67 NIST SP 800-53, Revision 4, controls specifically identified in the FY 2019 IG metrics. We tested the 66 that were applicable to systems within the scope of our audit. We also tested 2 additional privacy controls from Appendix J of NIST SP 800-53 Revision 4 because they related to the metrics. A control was counted for each system it was tested against. Thus, there were 157 instances of testing a control.

The audit also included a follow up on prior audit recommendations[13] to determine if USAID made progress in implementing the recommended improvements concerning its information security program. See Appendix IV for the status of prior year recommendations.

Audit fieldwork was performed at USAID's headquarters in Washington, DC, and Arlington, VA, from May 13, 2019, to October 24, 2019. It covered the period from October 1, 2018, through September 30, 2019.

Methodology

To determine if USAID implemented an effective information security program, CLA conducted interviews with USAID officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, CLA 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, CLA compared documents, such as USAID's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, CLA performed tests of system processes to determine the adequacy and effectiveness of those controls. Further, CLA reviewed the status of FISMA audit recommendations from fiscal year 2018.[14]

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

To perform our audit of USAID's information security program and practices, we followed a work plan based on the following guidance:

- OMB and DHS, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*
- OMB Circular Number A-130, *Managing Information as a Strategic Resource.*
- NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*.
- NIST SP 800-160, Revision 1, *Systems Security Engineering.*

[13] *USAID Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-19-005-C, November 21, 2018).
[14] Ibid. footnote 13.

MANAGEMENT COMMENTS

MEMORANDUM

TO: Alvin Brown, Deputy Assistant Inspector General (A/AIG)

FROM: Jay Mahanand, Chief Information Officer (CIO) /s/

DATE: January 3, 2020

SUBJECT: Management Comments to Respond to the Draft Report Produced by the Office of the Inspector General (OIG) titled, *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (A-000-20-00X-C).

The U.S. Agency for International Development (USAID) would like to thank the Office of the Inspector General (OIG) for the opportunity to provide comments on the subject draft report, *USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2019 in Support of FISMA* (A-000-20-00X-C). The Agency agrees with the seven recommendations, herein provides plans to implement them, and reports on significant progress already made.

Tab A—Management Decisions

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT ON THE DRAFT REPORT RELEASED BY THE OFFICE OF THE INSPECTOR GENERAL TITLED,
USAID HAS GENERALLY IMPLEMENTED CONTROLS IN SUPPORT OF FISMA FOR FISCAL YEAR 2019

Please find below the management decisions and corrective actions from the U.S. Agency for International Development (USAID) on draft report A-000-20-00X-C produced by the Office of the USAID Inspector General, which contains seven recommendations for the Agency:

Recommendation 1: USAID's [C]hief [I]nformation [O]fficer (CIO) should document and implement a process to confirm that approval of user access is documented prior to granting access to the system for which verbal approvals had been allowed.

- **Management Decision:** USAID agrees with the recommendation, and the Office of the CIO within the Bureau for Management (M) believes the Agency has taken sufficient action to address it. We have updated and implemented the *Account Management Procedures* for our systems (Tab B). Specifically, we have updated Section 4, *Account Creation,* to reflect that system administrators will not accept oral account requests, and that only a written, documented account request and approval process maintained by the system administrator can facilitate the request and approval of user accounts.

- **Target Date:** USAID requests the closure of this recommendation upon the issuance of the OIG's Final Report.

Recommendation 2: USAID's [C]hief [I]nformation [O]fficer should update its hardware-inventory policies to reflect the current operating environment.

- **Management Decision:** USAID agrees with the recommendation. M/CIO will update its hardware-inventory policies to reflect the current operating environment.

- **Target Completion Date:** September 30, 2020.

Recommendation 3: USAID's Senior [A]gency Official for Privacy should document and implement a process to continuously monitor and review privacy controls in accordance with the Privacy Continuous Monitoring Strategy.

- **Management Decision:** USAID agrees with the recommendation. M/CIO is currently assessing the USAID Privacy Common Control Catalogue and, moving forward, we will continue to review it in coordination with our annual continuous-monitoring activities.

- **Target Completion Date:** March 30, 2020.

Recommendation 4: USAID's [CIO] should update the System Security Plan to document the frequency with which position risk designations are to be reviewed and updated.

- **Management Decision:** USAID agrees with the recommendation, and M/CIO believes the Agency has taken sufficient action to address it. M/CIO has updated the Cyber Security Asset-Management (CSAM) tool to reflect the "Agency-defined control" for PS-2 (c) *Position Risk Designation,* to reflect a three-to-five-year review for Position Risk Designations (Tab C).

- **Target Date:** USAID requests the closure of this recommendation upon issuance of the OIG's Final Report.

Recommendation 5: USAID's [CIO] should document backup procedures for the current operating environment.

- **Management Decision:** USAID agrees with the recommendation, and M/CIO believes the Agency has taken sufficient action to address it. In Section 5.14 of the *Enterprise Data Center/Disaster Recovery (EDC/DR) Hybrid Cloud Technical Architecture and Design* document (Tab D), M/CIO has documented the Hybrid Cloud Storage and Backup process, which describes the storage and back-up services in Amazon Web Services (AWS) and co-location (COLO) for Hybrid Cloud.

- **Target Date:** USAID requests the closure of this recommendation upon the issuance of the OIG's Final Report.

Recommendation 6: USAID's [CIO] should update acquisition policies and procedures to include security requirements outlined in the *National Institute of Standards and Technology Special Publication 800-53, Revision 4, control SA 4—Acquisition Process,* for all information technology acquisitions.

- **Management Decision:** USAID agrees with the recommendation, and M/CIO believes the Agency has taken sufficient action to address it. Specifically, the Office of Acquisition and Assistance (OAA) within the M Bureau has documented and implemented *Acquisition and Assistance Policy Directive (AAPD) 16-02, Clauses and Special Contract Requirements for Facilities Access, Security, and Information Technology (IT)* (Tab E). AAPD 16-02 is the Agency's policy that reflects the clauses and language that all USAID contracts must include. Specifically, Section J(1) *Security Requirements,* states, "[T]he Contractor shall adopt and maintain administrative, technical, operational, and physical safeguards and controls that meet or exceed requirements contained within the Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline, current standard for [National Institute of Standards and Technology] NIST 800-53 (Security and Privacy Controls for Federal Information Systems) and Organizations, including Appendix J, and FedRAMP Continuous Monitoring Requirements for the security level and services being provided, in accordance with the security categorization or impact level as defined by the government based on the Federal Information Processing Standard (FIPS) Publication 199 (FIPS-199)"

- **Target Date:** USAID requests the closure of this recommendation upon the issuance of the OIG's Final Report.

Recommendation 7: USAID's [CIO] should conduct a documented review of National Institute of Standards and Technology [NIST] Special Publication 800-160, Revision 1, to identify security engineering principles that are applicable to the Agency and update the Agency's [System Development Life Cycle] SDLC Process Description Document accordingly.

- **Management Decision:** USAID agrees with the recommendation, and M/CIO believes the Agency has taken sufficient action to address it. M/CIO has updated and implemented the *System Development Life Cycle - Agile (SDLC-Agile) Process Description Document* (Tab F), which details the process activities, interfaces, and process inputs/outputs for the Agency SDLC process. Updated in Section 1.4 of this document, *References,* is additional information that supplements this guidance, including Waterfall and Agile SDLC Artifact

Lists/Responsible, Accountable, Consulted, Informed (RACI) Matrices, located on the internal Project Management Office (PMO) website. Additionally, we have updated Section 2.3, *Roles and Responsibilities,* to address responsibilities for the Development Team, consistent with NIST Special Publication 800-161, Revision 1, Security Engineering Principles. These include the following:

Development Team **Core Team** ● Business Analysts; ● Developers; ● Testers; ● Data-Specialists; and ● User Interface (UI) Developers. **Extended Team** ● Subject-Matter Experts, as needed; ● Database Administrators (DBAs); ● Architect; ● Security Engineer; and ● User-Experience (UX) Experts	● Develops User Stories; ● Includes User Stories in the Sprint Backlog; ● Ensures the finalization of a Definition of "Done" for User Stories, Sprints, and Releases; and ● Develops features in compliance with security design principles and concepts, including protection needs or constraints, architecture and design decisions and trade-offs, or by changes in risk tolerance, to ensure the incorporation of related-security standards in the total system solution.

- **Target Date:** USAID requests the closure of this recommendation upon the issuance of the OIG's Final Report.

In view of the above, we request that the OIG inform USAID when it agrees or disagrees with a management comment.

SUMMARY OF CONTROLS REVIEWED

Control	Control Name	Number of Systems Tested
AC-1	Access Control Policy and Procedures	6
AC-17	Remote Access	3
AC-2	Account Management	5
AC-8	System Use Notification	2
AR-1	Governance and Privacy Program	1
AR-2	Privacy Impact and Risk Assessment	1
AR-4	Privacy Monitoring and Auditing	3
AR-5	Privacy Awareness and Training	2
AT-1	Security Awareness and Training Policy and Procedures	1
AT-2	Security Awareness Training	1
AT-3	Role-Based Security Training	1
AT-4	Security Training Records	1
CA-1	Security Assessment and Authorization Policies and Procedures	2
CA-2	Security Assessments	6
CA-3	System Interconnections	3
CA-5	Plan of Action and Milestones	2
CA-6	Security Authorization	6
CA-7	Continuous Monitoring	5
CM-1	Configuration Management Policy and Procedures	2
CM-10	Software Usage Restrictions	1
CM-2	Baseline Configuration	4
CM-3	Configuration Change Control	4
CM-6	Configuration Settings	4
CM-7	Least Functionality	4
CM-8	Information System Component Inventory	6
CM-9	Configuration Management Plan	2
CP-1	Contingency Planning Policy and Procedures	2
CP-2	Contingency Plan	4
CP-3	Contingency Training	2
CP-4	Contingency Plan Testing	4
CP-6	Alternate Storage Site	1
CP-7	Alternate Processing Site	2
CP-8	Telecommunication Services	2
CP-9	Information System Backup	2
IA-1	Identification and Authentication Policy and Procedures	2
IR-1	Incident Response Policy and Procedures	1
IR-4	Incident Handling	1
IR-6	Incident Reporting	1

Control	Control Name	Number of Systems Tested
IR-7	Incident Response Assistance	1
MP-3	Media Marking	1
MP-6	Media Sanitization	1
PL-2	System Security Plan	6
PL-4	Rules of Behavior	1
PL-8	Information Security Architecture	4
PM-11	Mission/Business Process Definition	1
PM-5	Information System Inventory	1
PM-7	Enterprise Architecture	1
PM-8	Critical Infrastructure Plan	1
PM-9	Risk Management Strategy	1
PS-1	Personnel Security Policy and Procedures	1
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	2
RA-2	Security Categorization	4
RA-3	Risk Assessment	1
SA-3	System Development Life Cycle	4
SA-4	Acquisition Process	3
SA-8	Security Engineering Principles	3
SA-9	External Information System Services	2
SC-28	Protection of Information at Rest	2
SC-8	Transmission Confidentiality and Integrity	2
SE-2	Privacy Incident Response	2
SI-2	Flaw Remediation	3
SI-3	Malicious Code Protection	1
SI-4	Information System Monitoring	2
SI-7	Software, Firmware, and Information Integrity	1

STATUS OF PRIOR YEAR FINDINGS

The following table provides the status of the FY 2018 FISMA audit recommendations.[15]

FY 2018 Recommendation	USAID Position on Status	Auditor's Position on Status
1. We recommend that USAID's Chief Information Officer update the Agency's Vulnerability Management Standard Operating Procedure to (1) define the timeframe for applying system patches and (2) document and implement a process to validate that system patches are applied according to the timeframe specified in the procedure.	Closed	Disagree, see finding 1.
2. We recommend that USAID's Chief Information Officer document and implement a process to validate that unsupported software is either upgraded or removed within 48 hours of identification, as specified in the Agency's Unauthorized/Unsupported Software Standard Operating Procedures, or document acceptance of the risk for allowing the unsupported software on the network.	Closed	Disagree, see finding 1.
3. We recommend that USAID's Chief Information Officer document and implement a process to fully automate the disabling of accounts after 90 days of inactivity and document the results.	Closed	Agree
4. We recommend that USAID's Chief Information Officer document and implement a process to validate that Agency account management policies are enforced for all USAID information systems, or formally document acceptance of the risk when implementing the account management policies is not feasible.	Closed	Agree
5. We recommend that USAID's Chief Information Officer document and implement a process to validate that USAID procedures are followed for testing, conducting security impact analysis of, and approving system changes.	Closed	Disagree, see finding 3.

[15] *USAID Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-19-005-C, November 21, 2018).

FY 2018 Recommendation	USAID Position on Status	Auditor's Position on Status
6. We recommend that USAID's Chief Information Officer document and implement a process to validate that security assessment plans are documented and uploaded into the Cyber Security Assessment and Management tool.	Closed	Agree
7. We recommend that USAID's Chief Information Officer document and implement a process for reviewing plans of action and milestones on a regular basis to validate that scheduled completion dates, milestone updates, and quarterly updates are documented.	Closed	Agree
8. We recommend that USAID's Chief Information Officer document and implement a process to validate that USAID's privacy plan, policies, and procedures define personally identifiable information in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-122, and are reviewed and kept up-to-date at least on a biannual basis as recommended by NIST Special Publication 800-53 (revision 4).	Closed	Agree
9. We recommend that USAID's Chief Information Officer document and implement a process to complete the rollout of the role-based security training to all required individuals.	Closed	Agree