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

USAID Generally Implemented an Effective Information Security Program for Fiscal Year 2018 in Support of FISMA

AUDIT REPORT A-000-19-005-C
NOVEMBER 21, 2018

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, U.S. African Development Foundation, Inter-American Foundation, Millennium Challenge Corporation, 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 20044-065

MEMORANDUM

DATE: November 21, 2018

TO: 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 2018 in Support of FISMA (A-000-19-005-C)

Enclosed is the final audit report on USAID's information security program for fiscal year 2018, as required by the Federal Information Security Modernization Act of 2014 (FISMA). The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (Clifton) to conduct the audit. The contract required Clifton to perform the audit in accordance with generally accepted government auditing standards.

In carrying out its oversight responsibilities, OIG reviewed Clifton'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. Clifton is responsible for the enclosed auditor's report and the conclusions expressed in it. We found no instances in which Clifton 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, Clifton 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." Clifton auditors reviewed 6 of the 47 information systems in USAID's inventory dated December 2017. Fieldwork took place at USAID's headquarters in Washington, DC, from April 26 to September 11, 2018.

[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 found that USAID generally implemented an effective information security program by implementing 120 of 135 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 the controls USAID implemented or maintained were the following:

- A plan to confirm that all internal and external systems are currently authorized to operate
- A plan to assess system risks for all internal and external systems annually in accordance with Agency policy
- A procedure to review and analyze remote access connections
- An effective incident handling and response program
- An effective contingency planning program

The audit firm also identified weaknesses. For example, as summarized in the table below, Clifton noted weaknesses in 15 selected security controls that fall within 6 of the 8 IG FISMA metric domains.[2] These weaknesses increase USAID's information and information systems' vulnerability to unauthorized access, use, disclosure, disruption, modification, or destruction.

Fiscal Year 2018 IG FISMA Metric Domains	**Weaknesses Identified**
Risk Management	X
Configuration Management	X
Identity and Access Management	X
Data Protection and Privacy	X
Security Training	X
Information Security Continuous Monitoring	X
Incident Response	
Contingency Planning	

To address the weaknesses identified in the report, we recommend that USAID's chief information officer:

Recommendation 1. 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.

Recommendation 2. Document and implement a process to validate that unsupported software is either upgraded or removed within 48 hours of identification, as specified in the

[2] Each year inspectors general are required to complete metrics to independently assess their agencies' information security programs. The requirements for 2018 are in the following publication: Office of Management and Budget, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency, "FY 2018 Inspector General Federal Information Security Modernization Act for 2014 (FISMA) Reporting Metrics," May 24, 2018.

Agency's Unauthorized/Unsupported Software Standard Operating Procedures, or document acceptance of the risk for allowing the unsupported software on the network.

Recommendation 3. Document and implement a process to fully automate the disabling of accounts after 90 days of inactivity and document the results.

Recommendation 4. 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.

Recommendation 5. Document and implement a process to validate that USAID procedures are followed for testing, conducting security impact analysis of, and approving system changes.

Recommendation 6. Document and implement a process to validate that security assessment plans are documented and uploaded into the Cyber Security Assessment and Management tool.

Recommendation 7. 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.

Recommendation 8. 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).

Recommendation 9. Document and implement a process to complete the rollout of the role-based security training to all required individuals.

In finalizing the report, Clifton evaluated USAID's responses to the recommendations. After reviewing that evaluation, we consider recommendations 4, 5, 8, and 9 resolved but open pending completion of planned activities and recommendations 1, 2, 3, 6, and 7 resolved but open pending OIG's verification of the Agency's final action, which will take some additional time because we will contract out the testing and verification.

For recommendations 4, 5, 8, and 9, please provide evidence of final action to the Audit Performance and Compliance Division.

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

CliftonLarsonAllen

The Audit of USAID's Compliance with the Federal Information Security Modernization Act of 2014

Fiscal Year 2018

Final Report

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

November 7, 2018

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 is pleased to present the final version of our report on the United States Agency for International Development's (USAID) compliance with the Federal Information Security Modernization Act of 2014.

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 you may have.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen

CliftonLarsonAllen LLP
www.cliftonlarsonallen.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) compliance 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 six of USAID's internal information systems. Audit fieldwork was performed at USAID's headquarters in Washington, DC, from May 15, 2018 to September 11, 2018.

Our audit was performed in accordance with the performance audit standards specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. 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 objectives.

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 6 of the 8 Inspector General FISMA Metric Domains and have made nine recommendations to assist USAID in strengthening its information security program.

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

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
November 7, 2018

TABLE OF CONTENTS

Summary of Results 1

Audit Findings 4

USAID Needs to Strengthen Vulnerability Management Controls 4

USAID Needs to Strengthen Account Management Controls 5

USAID Needs to Strengthen Configuration Management Controls 8

USAID Needs to Conduct Proper Planning When Performing Security Control Assessments 9

USAID Needs to Strengthen Plan of Action and Milestones Controls 10

USAID Needs to Ensure Privacy Program Documentation is Completed and Maintained 12

USAID Needs to Implement Role Based Security Training 13

Evaluation of Management Comments 15

Appendix I – Scope and Methodology 17

Appendix II – Management Comments 19

Appendix III – Summary of Results of Each Control Reviewed 24

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. 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 16, 2017, OMB issued Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete 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) amends 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] The IG FISMA metrics will be completed as a separate deliverable.

The fiscal year (FY) 2018 metrics are designed to assess the maturity[4] of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover, as highlighted in Table 1.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2018 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2018 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 metrics from 6 of 47 information systems[6] in USAID's FISMA inventory as of December 2017.

The audit was performed in accordance with performance audit standards in *Government Auditing Standards*. 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 120 of 135 selected security controls for selected information systems. For example, USAID:

- Implemented a plan to confirm that all internal and external systems were authorized to operate.
- Implemented a plan to annually assess system risks for all internal and external systems in accordance with Agency policy.
- Implemented a procedure to review and analyze remote access connections.
- Maintained an effective incident handling and response program.
- Maintained an effective contingency planning program.

[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.

[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.

Although USAID generally implemented an effective information security program, its implementation of 15 of the 135 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. As a result, CLA noted weaknesses in the following FISMA Metric Domains (Table 2) and made nine recommendations to assist USAID in strengthening its information security program.

Table 2: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2018 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains	Weaknesses Noted in FY 2018
Identify	**Risk Management**	USAID Needs to Strengthen Vulnerability Management Controls (**Finding 1**) USAID Need to Strengthen POA&M Management Controls (**Finding 5**)
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**)
	Data Protection and Privacy	USAID Needs to Ensure Privacy Program Documentation is Completed and Maintained (**Finding 6**)
	Security Training	USAID Needs to Implement Role Based Security Training (**Finding 7**)
Detect	**Information Security Continuous Monitoring**	USAID Needs to Conduct Proper Planning When Performing Security Control Assessments (**Finding 4**)
Respond	**Incident Response**	No weaknesses noted.
Recover	**Contingency Planning**	No weaknesses noted.

We acknowledge USAID's management decisions on all nine recommendations. Based on our evaluation of the Agency's comments, we consider recommendations 4, 5, 8, and 9 resolved but open pending completion of planned activities. In addition, we consider recommendations 1, 2, 3, 6, and 7 resolved, but open pending OIG's verification of the Agency's final actions.

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 Management Controls

Cybersecurity Framework Security Function: *Identify*
FY 18 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;
> 9. Implement and maintain current updates and patches for all software and firmware components of information systems.

Additionally, the USAID *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. Additionally, USAID's *Vulnerability Management Standard Operating Procedure* did not address timeframes for applying patches.

[7] USAID performed the vulnerability scans during April 2018.

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. Therefore, CLA is making the following recommendations.

> ***Recommendation 1:*** *USAID's Chief Information Officer should 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.*
>
> ***Recommendation 2:*** *USAID's Chief Information Officer should 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.*

2. USAID Needs to Strengthen Account Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 18 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].
>
> * * *
>
> h. Notifies account managers:
>
> 1. When accounts are no longer required;
> 2. When users are terminated or transferred; and
> 3. When individual information system usage or need-to-know changes.

USAID's Automated Directives System (ADS) Chapter 545, *Information Systems Security*, Section 545.3.8.4 Identification and Authentication, states "(4) System Owners (SOs) must disable user identifiers after ninety (90) days of inactivity."

In addition, ADS Chapter 545, Section 545.3.2.2 Account Management, states "All SOs, Information Owners (IOs), and Bureaus must coordinate with ISSOs or M/CIO to establish a process to notify account managers when:

a. Accounts are no longer required,
b. Users are terminated or transferred, and
c. Individual information system usage or need-to-know changes occur."

ADS Chapter 545, Section 545.3.2.2 Account Management, additionally states, "(j) review accounts for compliance with account management requirements semi-annually."

Controls were not adequate to ensure USAID performed effective account management for five of six sampled systems. Specifically, CLA noted the following account management control weaknesses for inactive and terminated users, and a lack of periodic reviews.

For one sampled system, CLA noted the following issues:

- The process for disabling inactive accounts was not automated as required by NIST's Federal Information Processing Standard 199 for moderate and high systems. The last logon date for users connecting remotely also does not update in active directory. Management indicated they had not implemented automated account disabling because there were difficulties for users who primarily use remote access as their main connection to one system. However, management indicated they are developing a solution that will allow a fully automated solution to be implemented. To address a prior year audit recommendation[8] related to inactive accounts, USAID developed and implemented a process of running an automated script and closed the recommendation. However, CLA is issuing a new recommendation because the script that is run requires a manual intervention before accounts are disabled, and is therefore not fully automated.
- Of 527 privileged user accounts, 41 were not disabled after 90 days of inactivity. Additionally, 54 privileged user accounts never logged on and were not disabled. Management indicated the privileged accounts were excluded from the script used to identify accounts that have been inactive for 90 days or more, but they will update the script to include all privileged user accounts.
- USAID's review of privileged user accounts only included a subset of accounts on a quarterly basis, which may not include all accounts on a semi-annual basis. Management also did not have a process in place to maintain adequate evidence to show the review was performed, including what accounts were reviewed and what actions were taken as a result of the review.
- Of 687 non-privileged user accounts that were managed by an office other than the Office of the Chief Information Officer, 17 were not disabled after 90 days of inactivity. Management stated that accounts are created for users the day they on board; however, these users do not always need their account immediately. Additionally, management stated the accounts were required to be disabled after one year of inactivity, which contradicted ADS 545. Upon notification of the issue, management indicated they would conform to ADS 545 and will be disabling

[8] Recommendation 7, *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-18-003-C, October 6, 2017).

accounts that have been inactive for greater than 90 days. In addition, management specified that they are developing policies to create accounts in a disabled state and only enable the account once a user requires it.

For a second sampled system, management did not provide evidence of account recertification for privileged user accounts. Management did not have a process in place to maintain adequate evidence to show the review was performed, including what accounts were reviewed and what actions were taken as a result of the review.

For a third sampled system, CLA noted the following issues:

- The entire sample of 1 new privileged user from a population of 13 had access that was not approved. Specifically, the user had a role labeled Agency level system administrator access, but there was no documented approval for such access.
- From a sample of 25 separated users from the total population of 512, 6 accounts were not disabled upon separation. Management did not disable accounts because single sign on was enabled. Although the network accounts associated with the six accounts were disabled, there is still a risk to leaving dormant accounts active.
- Out of 12,284 enabled user accounts, 3,457 user accounts were not disabled after 90 days of inactivity; and 2,681 user accounts never logged in and were not disabled. Management did not disable user accounts after 90 days of inactivity because not all users regularly travel and require access. Management made the decision to not disable accounts due to inactivity, but did not formally document this decision and evaluate the associated risks.
- Agency officials could not provide evidence that they had performed semi-annual reviews of accounts. Management did not have a process in place to maintain adequate evidence to show the review was performed, including what accounts were reviewed and what actions were taken as a result of the review.

Of 397 enabled user accounts for a fourth sampled system, 134 were not disabled after 90 days of inactivity. Management did not perform reviews to ensure that all accounts that were inactive for over 90 days were disabled. In addition, Agency officials could not provide evidence that they had performed semi-annual reviews of the system’s accounts. Management did not have a process in place to maintain adequate evidence to show the review was performed, including what accounts were reviewed and what actions were taken as a result of the review.

Of 2,315 enabled user accounts for a fifth sampled system, 3 were not disabled after 90 days of inactivity. This occurred because the user access process required accounts to be disabled after 120 days of inactivity, which does not conform to ADS 545 requirements. In addition, Agency officials could not provide evidence that they had performed semi-annual reviews of the system’s accounts. Management did not have a process in place to maintain adequate evidence to show the review was performed, including what accounts were reviewed and what actions were taken as a result of the review.

Without effective access controls, USAID information is at risk of unauthorized access, increasing the likelihood of unauthorized modification, loss, and disclosure. Inactive accounts that are not disabled in accordance with Agency policy and user accounts that are not disabled when employees separate may be used to gain access to the Agency's data and sensitive information. In addition, the lack of comprehensive periodic account reviews can lead to system users with greater access than is required to perform their job functions and/or segregation of duties issues. Therefore, CLA is making the following recommendations.

> ***Recommendation 3:*** *USAID's Chief Information Officer should establish a process to fully automate the disabling of accounts after 90 days of inactivity and document the results.*
>
> ***Recommendation 4****: USAID's Chief Information Officer should 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.*

3. USAID Needs to Strengthen Configuration Management Controls

Cybersecurity Framework Security Function: *Protect*
FY 18 FISMA IG Metric Domain: *Configuration Management*

NIST SP 800-53, Revision 4, security control CM-3, states the following regarding configuration change control:

> The organization:
> ...
> b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.

In addition, CM-3 Control Enhancement (2) states: "The organization tests, validates, and documents changes to the information system before implementing the changes on the operational 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 Chapter 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's *Infrastructure Change Management Standard Operating Procedure* states:

> Expedited Change Requests go through a 'Virtual Review' process. This process is completed by either the Operation & Maintenance (O&M) Infrastructure Change Manager or the O&M Change Management Service Delivery Manager and consists of sending a standard email to the Permanent Voting Members, the Technical Review Board (TRB) and Change Control Board (CCB) Chairs requesting and Expedited, Virtual Review.

Contrary to the above procedures, USAID did not follow its change management procedures for two of six systems tested for the approval and testing of changes and for assessing security risks of the system changes. Specifically, CLA noted the following change management weaknesses.

- All 25 sampled change requests for one sampled system, from a total population of 666 change requests, did not have evidence that a security impact analysis was performed. In addition, 3 of the 25 change requests were emergency changes that did not have TRB/CCB approval. Management indicated that there were members from the Information Assurance team at the TRB and CCB meetings when they reviewed and assessed the security impact of changes. However, management was unable to provide documentation to show what security impacts were considered.

- For another sampled system, of the 17 change requests, 2 of 4 sampled did not have test plans or test results documented. While management indicated that all changes are planned and tested before implementation in the production environment, evidence of the test plans and test results was not provided.

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

> ***Recommendation 5:*** *USAID's Chief Information Officer should document and implement a process to validate that USAID procedures are followed for testing, conducting security impact analysis of, and approving system changes.*

4. USAID Needs to Conduct Proper Planning When Performing Security Control Assessments

Cybersecurity Framework Security Function: *Detect*
FY 18 FISMA IG Metric Domain: *Information System Continuous Monitoring*

NIST SP 800-53, Revision 4, security control CA-2, states the following regarding conducting security control assessments:

> The organization:
> * * *
>
> a. Develops a security assessment plan that describes the scope of the assessment including:
>   1. Security controls and control enhancements under assessment;
>   2. Assessment procedures to be used to determine security control effectiveness; and
>   3. Assessment environment, assessment team, and assessment roles and responsibilities.

In addition, ADS Chapter 545 Section 545.3.5.2, states:

> Security assessors, including independent assessors or self-assessors, must develop a security assessment plan that describes the scope of the assessment, including:
>
> a. Security controls and enhancements in scope;
> b. Assessment procedures; and
> c. Assessment environment, team, and roles and responsibilities.

USAID did not have a documented security assessment plan for the one sampled system's security assessment conducted in June 2017. Management stated this happened because the contractor who performed the assessment did not upload the assessment plan into the Cyber Security Assessment and Management tool.

A security assessment plan specifies the objectives of the assessment, the resources required to perform the assessment, and the assessment procedures. Without having a documented security assessment plan, the assessment may not align with the security objectives of the Agency, and proper resources and procedures may not be used to determine security control effectiveness. Therefore, CLA is making the following recommendation.

> ***Recommendation 6:*** *USAID's Chief Information Officer should document and implement a process to validate that security assessment plans are documented and uploaded into the Cyber Security Assessment and Management tool.*

5. USAID Needs to Strengthen Plan of Action and Milestones Controls

Cybersecurity Framework Security Function: *Identify*
FY 18 FISMA IG Metric Domain: *Risk Management*

NIST SP 800-53, Revision 4, security control CA-5, states the following regarding the management of plan of action and milestones (POA&M):

> The organization:
> * * *

> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
> b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

ADS 545, Section 545.3.5.4, states:

> SOs [system owners] must develop POA&Ms to document the planned remedial actions, and update the POA&Ms at least quarterly based on security monitoring activities. SOs must ensure that information security requirements and POA&Ms are adequately funded, resourced, and documented in accordance with current OMB budgetary guidance.

USAID did not follow proper POA&M management procedures for three of six sampled systems. Specifically, CLA noted the following POA&M management weaknesses:

- Five security controls identified as "Other Than Satisfied" in one sampled system's Security Assessment Report, dated May 10, 2018, were not documented as control weaknesses in the POA&Ms. Management specified that additional evidence was provided to the evaluation team during the security control assessment fieldwork to satisfy the controls; therefore the POA&Ms were never created. However, USAID could not provide documentation to validate that the assessment team reviewed and accepted the additional evidence. Additionally, from the total population of 16 open POA&Ms:
  - 1 did not have a scheduled completion date documented.
  - 12 missed the scheduled completion date and a new milestone completion date was not documented.
  - 12 were not updated on a quarterly basis, as required by USAID policy.

- The total population of one open POA&M for a second sampled system and three open POA&Ms for a third sampled system missed the scheduled completion dates and updated milestone dates were not documented. Although the root cause of this weakness could not be determined, management indicated that proper procedures were not followed when managing open POA&Ms.

POA&Ms are used by the authorizing official to evaluate corrective action plans and estimated timeframes for remediation of control weaknesses, and to monitor the progress of remediation. The lack of proper completion and updating of POA&Ms to reflect their current status affects USAID's ability to effectively manage security risks associated with their systems. Therefore, CLA is making the following recommendation.

> ***Recommendation 7:*** *USAID's Chief Information Officer should 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.*

6. USAID Needs to Ensure Privacy Program Documentation is Completed and Maintained

Cybersecurity Framework Security Function: *Protect*
FY 18 FISMA IG Metric Domain: *Data Protection and Privacy*

NIST SP 800-53, Revision 4, security control AR-1, states the following regarding an organizational privacy plan, policies, and procedures:

> The organization:
> a. Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].

In addition, NIST SP 800-53, Revision 4, security control AR-2, states the following regarding Privacy Impact Assessments:

> The organization:
> a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
> b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Furthermore OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, states, "the PIA document and, if prepared, summary, are made publicly available."

Finally, according to NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* PII is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Section 2.2, Examples of PII Data, states examples of PII data may include email addresses and business phone numbers.

The *USAID Privacy Program*, ADS Chapter 508, was not updated at least biennially as required by NIST. The Chapter also did not include a complete definition of personally identifiable information. The last review and revision was completed on September 15, 2014. Management indicated that updating policy level documentation requires extensive time and review and draft updates had been in process for a year.

Without an up-to-date privacy plan, privacy requirements and privacy and security controls that are in place or planned for meeting those requirements may not be documented, disseminated and implemented.

In addition, for a system that was decommissioned in June 2018, USAID did not complete the PIA even though the system collected PII. The system supported USAID's mission in their efforts to manage, monitor and report on their project portfolios. According to the privacy threshold analysis, the system collected first and last name, work phone number and work email address for authorized implementing partners to create user accounts. Management indicated that they did not consider the authorized implementing partners' names, work phone numbers and work email addresses PII and therefore, a PIA was not required.

Without the proper completion of PIAs, USAID may not be fully aware of all risks of collecting and maintaining PII, and protections for handling the information may not be fully implemented. In addition, without a PIA being publicly available, USAID did not communicate with the public about how the information was handled. Since the system was decommissioned a recommendation regarding the PIA is not being made. Regarding the privacy policy, CLA is making the following recommendation.

> ***Recommendation 8:*** *USAID's Senior Agency Official for Privacy should 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 in accordance with NIST Special Publication 800-53 (rev. 4).*

7. USAID Needs to Implement Role Based Security Training

Cybersecurity Framework Security Function: *Protect*
FY 18 FISMA IG Metric Domain: *Security Training*

NIST SP 800-53, Revision 4, security control AT-3, states the following regarding role-based security training:

> The organization provides role based security training to personnel with assigned security roles and responsibilities:
>
> a. Before authorizing access to the information system or performing assigned duties;
> b. When required by information system changes; and
> c. [Assignment: organization-defined frequency thereafter.

In addition, ADS Chapter 545 states:

> All USAID staff and others working on behalf of USAID with significant security responsibilities (i.e., ISSOs and SAs) must receive role-based training specific to their security responsibilities upon assignment to the role, and refresher training yearly thereafter. When access to an Information System is required by contract, the [Contracting Officer's Representative] must ensure that contractors complete the appropriate specialized training and

> refresher courses. Additional role-based training may be required as needed to address technology changes or patterns in threats and vulnerabilities in information systems.

From a population of 150 privileged users, 13 from a sample of 15 did not take role-based training. While USAID had determined the group of individuals that require role based training, USAID was still in the process of implementing the training and was rolling it out for its Information System Security Officers only this year.

Without role-based training, individuals responsible for system administration and security of USAID information systems may not maintain the knowledge required to perform their responsibilities. In addition, personnel may be performing tasks without proper training, thus potentially increasing the risk that the Agency's information and information systems could become compromised leading to unauthorized access, data loss, data manipulation and unavailability. Therefore, CLA is making the following recommendation.

Recommendation 9: *USAID's Chief Information Officer should document and implement a process to complete the roll out of the role-based security training to all required individuals.*

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, USAID outlined its plans to address all 9 recommendations. USAID's comments are included in their entirety in Appendix II.

Based on our evaluation of management's comments, we acknowledge management decisions on all 9 recommendations. In addition:

- For recommendations 4, 5, 8, and 9, USAID provided its corrective action plans to address the weaknesses. Therefore, we consider these recommendations resolved, but open pending completion of planned activities.
- For recommendations 1, 2, 3, 6, and 7, USAID requested closure upon issuance of the final report. However, there has not been sufficient time to determine if management has fully implemented its planned actions. Therefore, we consider those recommendations to be resolved, but open pending OIG's verification of the Agency's final action.

Below is our evaluation of management's request for closure for recommendations 1, 2, 3, 6, and 7.

For recommendation 1, we agree the *Vulnerability Management Standard Operating Procedure* has been updated. However, there has not been sufficient time to determine if management has implemented a process to validate that system patches are applied according the timeframe specified. Therefore, we consider recommendation 1 resolved but open pending OIG's verification of the Agency's final actions.

For recommendation 2, we agree the *Unauthorized/Unsupported Software Standard Operating Procedure* has been updated to define how unsupported software is either upgraded or removed after identification. However, there has not been sufficient time to determine if management has fully implemented the new process. Therefore, we consider recommendation 2 resolved but open pending OIG's verification of the Agency's final actions.

For recommendation 3, we acknowledge the script to disable accounts after 90 days of inactivity has been updated. However, there has not been sufficient time to determine if the updated script has been fully implemented and is working properly. Therefore, we consider recommendation 3 resolved but open pending OIG's verification of the Agency's final actions.

For recommendation 6, we agree the Certification Statement Template has been updated to require the assessor to confirm they have uploaded the required documentation in the Cyber Security Assessment and Management tool. However, there has not been sufficient time to assess whether USAID has fully implemented this new process. Therefore, we consider recommendation 6 resolved but open pending OIG's verification of the Agency's final actions.

For recommendation 7, we agree the *Plan of Action and Milestone (POA&M) Management Guide* has been updated to include new procedures for reviewing completion dates, milestone updates, and quarterly updates. However, there has not been sufficient time to determine if the process has been fully implemented. Therefore, we consider recommendation 7 resolved but open pending OIG's verification of the Agency's final actions.

SCOPE AND METHODOLOGY

Scope

CLA conducted this audit in accordance with performance auditing standards, as specified in the Government Accountability Office's *Government Auditing Standards*. 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. The audit was designed to determine whether USAID implemented an effective[9] 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
- 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, selected controls related to the FY2018 IG FISMA reporting metrics from 6 of 47 information systems in USAID's systems inventory as of December 2017 were reviewed. See Appendix III for a listing of selected controls.

The audit also included a follow up on prior audit recommendations[10] to determine if USAID made progress in implementing the recommended improvements concerning its information security program.

Audit fieldwork was performed at USAID's headquarters in Washington, D.C., and Arlington, VA, from April 26, 2018 to September 11, 2018.

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

[10] *USAID Has Implemented Controls In Support of FISMA, But Improvements Are Needed* (Audit Report No. A-000-18-003-C, October 6, 2017).

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. Also, 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. In addition, CLA reviewed the status of FISMA audit recommendations from fiscal year 2017.[11]

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.

[11] Ibid.

MANAGEMENT COMMENTS

The following is the full text of USAID's management comments on the draft report, excluding the attachments.

USAID
FROM THE AMERICAN PEOPLE

October 26, 2018

MEMORANDUM

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

FROM: Patrick Robinson, Deputy Chief Information Officer /S/
(For Jay Mahanand, Chief Information Officer)

SUBJECT: Management Response to the Audit of Compliance by the U.S. Agency for International Development (USAID) with the Federal Information Security Modernization Act (FISMA) of 2014 during Fiscal Year (FY) 2018 (Audit Report No. A-000-18-0XX-C, dated October 15, 2018): *USAID Has Generally Implemented Controls in Support of FISMA for Fiscal Year 2018*

Thank you for the opportunity to respond to the draft audit report produced by your office that assesses USAID's compliance with the FISMA during FY 2018. This letter contains USAID's Management Decisions to the recommendations contained in the draft report:

Recommendation 1: 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.

Management Decision: USAID agrees with the Recommendation, and Office of the CIO believes we have taken sufficient action to address it. We have updated and implemented the *USAID Vulnerability Management Standard Operating Procedure (SOP)* (Tab A). Specifically, Section 3.4 of this document addresses the time requirements and risk acceptance procedure for applying patches. This revised process defines the timelines for patching Information Technology (IT) products based on the severity of the vulnerability, and identifies specific actions for ensuring we have implemented the patches, or for taking approved alternative methods for instances in which we cannot apply patches within the required timelines. Alternate procedures include risk-acceptance and removal of the device from the network.

Target Date: USAID requests closure of this Recommendation upon the issuance of Audit Report A-000-18-0XX-C.

Recommendation 2: 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.

Management Decision: USAID agrees with the Recommendation, and the Office of the CIO believes we have taken sufficient action to address it. We have updated the *Unauthorized/Unsupported Software Standard Operating Procedure (SOP)* (Tab B) that details the process for properly handling and documenting unauthorized software on Agency staff workstations in support of USAID's security posture. Specifically, Section 6.0.1 of this document addresses the step-by-step action taken by the Office of the CIO's Security Operations (SecOps) in the event it detects unauthorized software. This includes opening a Service Desk ticket to track the incident, removing the software immediately, as well as contacting the workstation assignee or system manager. We perform this process on a monthly basis by pulling a list of software installed on all user machines and comparing it to the unapproved software list. We have completed a review of the *Disapproved Software List* (Tab C), as well as the *Approved Software List* (Tab D), and have validated that these lists accurately reflect USAID's software inventory, including software disapproved on our network.

Target Date: USAID requests closure of this Recommendation upon the issuance of Audit Report A-000-18-0XX-C.

Recommendation 3: A process to fully automate the disabling of accounts after 90 days of inactivity and document the results.

Management Decision: USAID agrees with the Recommendation, and the Office of the CIO believes we have taken sufficient action to address it. We have implemented a script (Tab E), which runs on a daily basis that automatically pulls a list of all active directory user objects across all USAID domains, and performs a check to determine if any user objects have been inactive for more than 80 days. The script automatically disables any objects that meet these criteria. We have intentionally set this script to check for 80 days of inactivity, instead of the 90 day inactivity requirement, in effort to provide a 10 day buffer for ensuring no accounts exceed the 90 day inactivity policy.

Target Date: USAID requests closure of this Recommendation upon the issuance of Audit Report A-000-18-0XX-C.

Recommendation 4: 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.

Management Decision: USAID agrees with the Recommendation. The Office of the CIO will implement a process to validate that we are enforcing the Agency's account management policies for all USAID's information systems, or document formally our acceptance of the risk when implementing the account management policies is not feasible.

Target Date: May 31, 2019.

Recommendation 5: A process to validate that USAID procedures are followed for testing, conducting security impact analysis of, and approving system changes.

Management Decision: USAID agrees with the Recommendation. The Office of the CIO will document and implement a process to validate that we are following USAID's procedures for testing, conducting a security impact analysis of, and approving system changes.

Target Date: March 31, 2019.

Recommendation 6: A process to validate that security assessment plans are documented and uploaded into the Cyber Security Assessment and Management tool.

Management Decision: USAID agrees with the Recommendation, and the Office of the CIO believes we have taken sufficient action to address it. Specifically, we have updated our *Certification Statement Template* (Tab F), which is a required document we complete for all System Security Assessment and Authorizations (SA&A) as part of our decision to grant Authorizations to Operate (ATOs). Appendix 4, Section B of this document requires the assessor who completes the SA&A to confirm the date he or she uploaded the Security Assessment Plan (SAP) to the Cyber Security Assessment and Management (CSAM) tool. The Certification Statement and SA&A will remain incomplete, and the Information Assurance (IA) Chief or the Chief Information Security Officer (CISO) will not sign them, unless documents affirm that the assessor has uploaded the SAP to CSAM.

Target Date: USAID requests closure of this Recommendation upon the issuance of Audit Report A-000-18-0XX-C.

Recommendation 7: 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.

Management Decision: USAID agrees with the Recommendation, and the Office of the CIO believes we have taken sufficient action to address it. M/CIO has updated and implemented the *Plan of Action and Milestone (POA&M) Management Guide* (Tab G), which includes the following procedures:

- A weekly notification sent automatically from CSAM to our Information System Security Officers (ISSO), System Owners (SO), and Security Compliance points of contact to alert them of upcoming and overdue POA&M dates (See Appendix E of the POA&M Management Guide);
- Monthly and yearly POA&M reviews by the Office of the CIO Governance team who works directly with system ISSOs;
- Monthly reports on POA&M status will be provided to the CISO and CIO;
    - Quarterly reporting from the ISSOs/SOs to the IA group that they have reviewed and updated POA&Ms;
    - The IA staff will review selected systems by the IA staff to ensure the effective management of POA&Ms;
    - When they detect problems, the IA staff will request a meeting with the relevant ISSO and SO to discuss remedial actions.

Target Date: USAID requests closure of this Recommendation upon the issuance of Audit Report A-000-18-0XX-C.

Recommendation 8: 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).

Management Decision: USAID agrees with the Recommendation. The office of the CIO will implement a process to validate that USAID's Privacy Plan, policies, and procedures define Personally Identifiable Information (PII) in accordance with NIST Special Publication 800-122, and to review and keep them up to date at least on a biannual basis, as recommended by NIST Special Publication 800-53 (revision 4). At the same time, the Agency will be revising the chapter of its Automated Directives System (ADS) that involve privacy (507 and 508) to reflect delegation of authority from the Administrator to the Inspector General to manage requests under the Privacy Act and the Freedom of Information Act. The confluence of these two processes means the Agency will need a few extra months to complete our implementation of Recommendation 8.

Target Date: March 31, 2019

Recommendation 9: A process to complete the rollout of the role-based security training to all required individuals.

Management Decision: USAID agrees with the Recommendation. The Office of the CIO will implement a process to complete the rollout of the role-based security training to all required individuals. We intend to ensure we have specific, role-based trainings customized for the data involved, and plan to introduce the courses during our normal annual window for Information Technology training, which ends on July 3, 2019.

Target Date: August 30, 2019.

Attachments:

Tab A: USAID Vulnerability Management SOP
Tab B: USAID SOPs for Unauthorized/Unsupported Software
Tab C: USAID List of Disapproved Software
Tab D: USAID List of Approved Software
Tab E: Script to Disable Inactive Accounts
Tab F: USAID System Certification Statement Template
Tab G: USAID POA&M Management Guide

Summary of Controls Reviewed

The following table identifies the controls selected for testing.

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

Control	Control Name	Number of Systems Tested
PL-8	Information Security Architecture	2
PM-11	Mission/Business Process Definition	1
PM-12	Insider Threat Program	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	2
PS-2	Position Risk Designation	1
PS-3	Personnel Screening	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	3
RA-2	Security Categorization	6
SA-3	System Development Life Cycle	3
SA-4	Acquisition Process	3
SA-8	Security Engineering Principles	2
SC-12	Cryptographic Key Establishment and Management	4
SE-2	Privacy Incident Response	2
SI-2	Flaw Remediation	2
SI-4	Information System Monitoring	2