



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

USAID Has Implemented Controls in Support of FISMA, but Improvements Are Needed

AUDIT REPORT A-000-18-003-C
OCTOBER 06, 2017

1300 Pennsylvania Avenue NW • Washington, DC 20523
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: ighotline@usaid.gov

Complaint form: <https://oig.usaid.gov/content/oig-hotline>

Phone: 202-712-1023 or 800-230-6539

Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657



MEMORANDUM

DATE: October 06, 2017

TO: Chief Information Officer, Jay Mahanand
Chief Human Capital Officer, Kimberly A. Lewis

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

SUBJECT: USAID Has Implemented Controls in Support of FISMA, but Improvements Are Needed (A-000-18-003-C)

Enclosed is the final audit report on the U.S. Agency for International Development's (USAID) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year 2017. 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 issued by the Comptroller General of the United States.

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 certain security controls for selected information systems in support of FISMA. To answer the audit objective, Clifton tested USAID's implementation of selected controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Clifton reviewed selected controls for three internal information systems and three external systems out of the total population of 45 systems in USAID's inventory as of March 27, 2017. The firm also performed a vulnerability assessment of USAID's general support system and an evaluation of USAID's process for

identifying, correcting, and mitigating technical vulnerabilities. Fieldwork was performed at USAID's headquarters in Washington, DC, and in Arlington, VA, from March 8, through August 24, 2017.

The audit firm concluded that USAID generally complied with FISMA requirements by implementing 150 of 162 selected security controls for selected information systems. For example, USAID did the following:

- Appointed a senior-level chief information security officer and segregated the duties of the deputy chief information officer and chief information security officer.
- Maintained an effective security awareness and training program for its employees.
- Maintained an effective incident handling and response program.
- Maintained an effective contingency planning program.
- Implemented an effective physical and environmental protection program at two USAID headquarters' locations.

However, Clifton found that USAID did not implement 12 controls designed to preserve the confidentiality, integrity, and availability of its information and information systems. To address the weaknesses identified in the report, Clifton made and OIG agrees with the following recommendations to USAID's management. We will track the recommendations until they are fully implemented. We recommend that:

Recommendation 1. The chief information officer document and implement a process to track and remediate persistent vulnerabilities, or document acceptance of the associated risks.

Recommendation 2. The chief information officer document and implement a process to verify that vulnerability assessment tools are configured to detect vulnerabilities previously undiscovered by internal scans.

Recommendation 3. The chief information officer develop and implement a documented process to migrate unsupported applications from their existing platform to vendor-supported platforms. The risk and approval, including adequate compensating controls, should be documented if an exception must be made until the unsupported software is migrated to vendor-supported platforms.

Recommendation 4. The chief information officer document and implement a process to verify that Microsoft Windows systems comply with the U.S. Government Configuration Baseline, and to grant and disseminate approved deviations from the baseline configuration settings.

Recommendation 5. The chief information officer document and implement a plan to confirm all internal and external systems are currently authorized to operate.

Recommendation 6. The chief information officer document and implement a plan to annually assess risks for all internal and external systems in accordance with agency policy.

Recommendation 7. The chief information officer establish a process to monitor the operation of the automated script that disables accounts after 90 days of inactivity.

Recommendation 8. The chief information officer (a) identify system owners; (b) require them to verify their procedures for revoking system access accounts for separated and transferred employees and contractors are enforced; and (c) document their responses.

Recommendation 9. The chief information officer document and implement a procedure to check for unauthorized software at established intervals.

Recommendation 10. The chief human capital officer document and implement a process to verify that all employees' exit clearance forms are completed and maintained in accordance with policy.

Recommendation 11. The chief information officer document and implement a procedure to review and analyze remote access connections.

In finalizing the report, Clifton evaluated USAID's responses to the recommendations. Both Clifton and OIG consider recommendation 8 closed, and recommendations 1 through 7 and 9 through 11 resolved but open pending completion of planned activities.

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



**The United States Agency for International Development Has
Implemented Many Controls in Support of the Federal Information
Security Modernization Act of 2014, but Improvements Are Needed**

Fiscal Year 2017

Final Report



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

October 4, 2017

Mr. Mark S. 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:

Enclosed is 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 (FISMA), *The United States Agency for International Development Has Implemented Many Controls in Support of the Federal Information Security Modernization Act of 2014, but Improvements Are Needed*. The USAID Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP to conduct the audit in support of the FISMA requirement for an annual evaluation of USAID's information security program.

The objective of this performance audit was to determine whether USAID implemented certain security controls for selected information systems in support of FISMA. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology (NIST) 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 (three internal and three external systems) out of the total population of 45 USAID information systems as of March 27, 2017. The audit also included a vulnerability assessment of USAID's general support system and an evaluation of USAID's process for identifying and correcting/mitigating technical vulnerabilities. The audit fieldwork was performed at USAID's headquarters in Washington, D.C. and Arlington, VA, from March 8, 2017, through August 24, 2017.

Our audit was performed in accordance with *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.

The audit concluded that USAID generally complied with FISMA by implementing 150 of 162 security controls reviewed for selected information systems. Although USAID generally had policies for its information security program, its implementation of those policies for 12 of 162 security controls was not fully effective to preserve the confidentiality, integrity, and availability of USAID's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in USAID's information security program that needed to be improved. We are making eleven recommendations to assist USAID in strengthening its information security program.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose.

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,

CLIFTONLARSONALLEN LLP

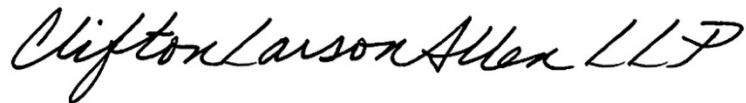
A handwritten signature in black ink that reads "Clifton Larson Allen LLP". The signature is written in a cursive, flowing style.

TABLE OF CONTENTS

Summary of Results	1
Audit Findings	4
1. USAID Needs to Strengthen Security Controls Surrounding Patch and Configuration Management.....	4
2. USAID Needs to Maintain Current System Authorizations to Operate and Assess System Risks.....	6
3. USAID Needs to Strengthen Account Management Controls.....	8
4. USAID Needs to Implement a Process to Monitor for Unauthorized Software.....	10
5. USAID Needs to Strengthen Personnel Out-Processing Procedures.....	11
6. USAID Needs to Monitor Remote Access Connections.....	12
7. Information System Agreements Need to be Current.....	13
8. USAID Needs to Implement Role Based Security Training.....	13
9. USAID Needs to Ensure Session Lock for Remote Access is Configured in Accordance with Agency Policy.....	14
Evaluation of Management Comments	16
Appendix I – Scope and Methodology	17
Appendix II – Management Comments	19
Appendix III – Summary of Controls Reviewed	25

SUMMARY OF RESULTS

The Federal Information Security Modernization Act of 2014¹ (FISMA), requires 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. Because the U.S. Agency for International Development (USAID) is a federal agency, it is required to comply with federal information security requirements.

The act also 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. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for Federal agencies.

The USAID Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP to conduct an audit in support of the FISMA requirement for an annual evaluation of USAID's information security program. The objective of this performance audit was to determine whether USAID implemented certain security controls for selected information systems² in support of FISMA.

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

For this audit, we reviewed selected controls for six information systems³ including general support systems⁴, major applications⁵, and external systems.⁶

¹ The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (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 See Appendix III for a summary of controls reviewed.

³ 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.

⁴ According to Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, a general support system means an interconnected set of information resources under the same direct management control which shares common functionality.

⁵ According to Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, a major application means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

⁶ According to NIST, an external system is an information system or component of an information system that is outside of the authorization boundary established by the organization and for which

Results

The audit concluded that USAID generally complied with FISMA requirements by implementing 150 of the 162 security controls reviewed⁷ for selected information systems (three internal and three external). For example, USAID:

- Appointed a senior-level chief information security officer and segregated duties of the deputy chief information officer and chief information security officer.
- Maintained an effective security awareness and training program for its employees.
- Maintained an effective incident handling and response program.
- Maintained an effective contingency planning program.
- Implemented an effective physical and environmental protection program at two headquarter's locations.

Although USAID generally had policies and procedures for its information security program, its implementation of those policies for 12 of the 162 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of USAID's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified several areas in USAID's information security program that needed to be improved. Specifically, USAID needs to:

- Strengthen patch and configuration management controls.
- Maintain current system authorizations to operate and assess system risks.
- Strengthen account management controls.
- Implement a process to check for unauthorized software.
- Strengthen personnel out-processing procedures.
- Monitor remote access connections.
- Maintain current information system agreements.
- Implement controls for role-based training.
- Verify the session lock control for remote access is configured in accordance with Agency policy.

the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

⁷ See Appendix III – Summary of Results of Each Control Reviewed.

Consequently, USAID's operations and assets are at risk of unauthorized access, misuse and disruption. We have made 11 recommendations to assist USAID in strengthening its information security program. In addition, findings related to one FY 2015⁸ and two FY 2016 recommendations⁹ were not fully implemented and therefore new recommendations were not made. (See pages 4 – 15)

Based on our evaluation of management comments, we acknowledge management decisions on all 11 recommendations for fiscal year 2017 and we agree with the final actions taken for recommendation 8.

Detailed findings appear in the following section. Appendix I describes the audit scope and methodology.

⁸ Recommendation 13, *Audit of USAID's Fiscal Year 2015 Compliance with the Federal Information Security Management Act Of 2002, as Amended* (Audit Report No. A-000-15-010-P), September 25, 2015).

⁹ Recommendations 13 and 17, *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-17-001-C, October 27, 2016).

AUDIT FINDINGS

1. USAID Needs to Strengthen Security Controls Surrounding Patch and Configuration Management

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control 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.

Office of Management and Budget, 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.

Independent scans of USAID's networks and a sample of four missions out of the total population of 64 identified critical and high risk security vulnerabilities related to patch management, configuration management, and unsupported software. In addition, a comparison of our independent scans and USAID's scans from the same time period identified several vulnerabilities that were not found in USAID's scans.

Management indicated that they faced several logistical issues in updating remote laptops for traveling personnel. Laptop owners may not have their laptops on the network long enough to receive all updates. Some owners may also have corrupted patch management client's software, which would prevent the laptop from receiving updates. In addition, patch management has been a distributed responsibility with local missions and site management.

USAID was also in the process of replacing the vulnerability scanning appliances with a vulnerability management tool and configuring it for USAID's purposes. In addition, the difference in scans may be due to the configuration variances of the scanners or the accounts used by USAID to perform the scans may not have the appropriate permissions to complete the scans. USAID management was actively working towards secure management and configuration of administrative accounts and privileged authentication.

Furthermore, information technology assets were not always centrally managed or hardened prior to being placed into the production environment. Management indicated that this was due to the assets not being properly setup before their deployment to end users.

We also found that USAID was not in compliance with their baseline configurations. A recent scan performed by USAID indicated 61% of Microsoft Windows systems failed the configuration audit for compliance with United States Government Configuration Baseline (USGCB)¹⁰ standards. However, USAID did not have approved deviations from baseline configurations documented. With the recent deployment of a vulnerability management tool, USAID is continuing to tailor baselines and deviations to their environment.

Unmitigated vulnerabilities on the USAID 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 the vendors have addressed with current supported versions and are no longer supported by the vendors against future vulnerabilities and exploits.

The fiscal year 2016 audit report made recommendations to address the weaknesses related to remediating vulnerabilities on the network and printer management;¹¹ however, procedures were not fully implemented and USAID had not closed the recommendations. Therefore, we are not making additional recommendations at this time regarding remediation weaknesses on the network and printer management.

¹⁰ The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security.

¹¹ Recommendations 4 and 7, *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-17-001-C, October 27, 2016).

Although USAID documented procedures for implementing a process to track and remediate persistent vulnerabilities and ensuring vulnerability assessment tools were configured to detect vulnerabilities, they had not fully implemented these procedures. Because USAID officially closed the recommendations,¹² we are issuing the following new recommendations to correct the weaknesses related to USAID's vulnerability management:

Recommendation 1: *We recommend that the chief information officer document and implement a process to track and remediate persistent vulnerabilities, or document acceptance of the associated risks.*

Recommendation 2: *We recommend that the chief information officer document and implement a process to verify that vulnerability assessment tools are configured to detect vulnerabilities previously undiscovered by internal scans.*

Recommendation 3: *We recommend that the chief information officer develop and implement a documented process to migrate unsupported applications from their existing platform to vendor-supported platforms. The risk and approval, including adequate compensating controls, should be documented if an exception must be made until the unsupported software is migrated to vendor-supported platforms.*

Recommendation 4: *We recommend that the chief information officer document and implement a process to verify Microsoft Windows systems comply with the U.S. Government Configuration Baseline and to grant and disseminate approved deviations from the baseline configuration settings.*

2. USAID Needs to Maintain Current System Authorizations to Operate and Assess System Risks

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

The organization:

* * *

- b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
- c. Produces a security assessment report that documents the results of the assessment; and
- d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].

¹² Recommendations 5 and 6, *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-17-001-C, October 27, 2016).

Furthermore, security control RA-3, states the following regarding risk assessment:

The organization:

* * *

- e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

In addition, security control CA-6, states the following regarding security authorization:

The organization:

* * *

- c. Updates the security authorization [Assignment: organization-defined frequency].

USAID *Automated Directives System (ADS) Chapter 545, Information Systems Security*, Section 545.3.3.12 Security Assessment and Authorization, states "(11) Systems must not be deployed as an operational system until they have received an Authorization to Operate (ATO) certified by the Chief Information Security Officer (CISO) and signed by the SO or AO."

The USAID *Information Security Continuous Monitoring Strategy*, Section 7.1.2 Implementation states the following regarding security control assessments:

USAID assesses all security controls employed within and inherited by information systems during the initial security authorization. Subsequent to the initial authorization, the Agency must assess a subset of the security controls on an ongoing basis during continuous monitoring.

USAID "Security Core Controls" are those controls that are most important to the organization and associated systems and should be assessed annually. The Agency also requires that at least one-third of the total system security controls to be assessed annually and each security control to be assessed at least once during every three year cycle.

The FY 2016 FISMA audit reported that ATOs had expired for five of 25 internal USAID systems and seven of 25 external systems.¹³ During fiscal year 2017, we noted that five of 25 internal systems had expired ATOs. Four of the five internal systems were the same systems as the prior year. In addition, we noted six of 21 external systems had expired ATOs. Four of the six external systems were the same as the prior year. Management indicated that the systems were either in process of completing their re-authorization, waiting on funding to do the re-authorization, awaiting decommissioning of the system, or looking for an outside vendor to assist with the assessment process.

In addition, USAID did not properly assess system risks for one application tested. Specifically, we noted that an annual assessment for that application was not performed.

¹³ Audit Finding 4, *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-17-001-C, October 27, 2016).

Management specified that the application received a one year ATO in May 2016 as a result of security assessment and authorization activities. Subsequently, a three month ATO extension was issued in May 2017. Due to priority placed on activities to correct deficiencies to achieve a longer term ATO, annual testing was not conducted.

By not completing continuous monitoring activities and assessing system risk, there is an increased risk that the Authorizing Official may not have the appropriate knowledge to ensure mitigation of known risks and make risk-based decision on whether to authorize the system to continue to operate. In addition, there is an increased risk that USAID systems are susceptible to risks of unauthorized access, viruses, malicious code, and exploitable vulnerabilities.

Although USAID documented procedures for implementing a process to track and authorize internal and external systems, they did not fully implement the process. Because USAID officially closed the recommendation addressing the weaknesses related to system ATOs that was made in the fiscal year 2016 audit,¹⁴ we are issuing the following new recommendation to correct this weakness:

Recommendation 5: *We recommend that the chief information officer document and implement a plan to confirm all internal and external systems are currently authorized to operate.*

Recommendation 6: *We recommend that the chief information officer document and implement a plan to annually assess system risks for all internal and external systems in accordance with agency policy.*

3. USAID Needs to Strengthen Account Management Controls

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 ADS Chapter 545, Section 545.3.5.1 Identification and Authentication, states “(4) System Owners (SOs) must disable user identifiers after ninety (90) days of inactivity.”

¹⁴ Recommendation 8, *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-17-001-C, October 27, 2016).

In addition, USAID ADS Chapter 545, Section 545.3.4.1 Personnel Security, *Separation From Duty*, states “(1) SOs must implement procedures to revoke access for USAID employees, contractors, or others working on behalf of USAID who leave the Agency, take up other duties, or no longer need access.”

The System Owner *User Management Guide*, dated March 29, 2017 states: “The system Point of Contact (POC)/Bureau Transition Coordinator (BTC) will email the system access team when system users have left the Mission or the Agency as well as people who no longer need system access. The access team will inactivate or deactivate the system ID depending on the circumstance. Once complete, the access team will notify the system POC/BTC.”

Controls were not adequate to ensure USAID performed effective account management for two systems tested. Specifically, we noted the following regarding account management controls for inactive and terminated users:

- Four accounts were not disabled after 90 days of inactivity for one system tested. Specifically, these accounts had not logged on for 95 to 365 days and were not disabled. USAID management indicated there was an error with the operation of the automated script to disable accounts after 90 days of inactivity. In addition, we identified five employees and one contractor who separated, and their accounts were not disabled for the same system. These employees had separated from USAID between 11 to 171 days and the contractor had separated from USAID for 49 days. Management specified the Chief Information Officer (CIO) Office and system owners did not consistently receive separation information from Human Resources, Contracting Officer Representatives and Administrative Management Staff Officers that would be required to assure system accounts were disabled when the employees and contractors separated.
- From a sample of 25 separated employees from the total population of 341, one employee’s account was not disabled for another system tested. This employee had separated from USAID for 81 days at the time testing occurred. USAID did not follow the system owner user management procedures for deactivating system accounts for separated users. USAID management indicated BTCs and POCs did not notify the system access team that the employee had separated. In addition, management indicated compensating controls related to single sign on¹⁵ and the automated disabling of accounts after 90 days of inactivity were in place. However, there is a possibility that active dormant accounts can be mishandled and misused, increasing the risk of unauthorized or improper access.

¹⁵ Single sign on is an authentication process that allows users access to multiple systems with one set of log on credentials.

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 misused or susceptible to a 'brute force' attack to gain access to the agency's data and sensitive information.

A recommendation addressing the weakness related to separated employees and contractors was made in the fiscal year 2016 audit;¹⁶ however, procedures were not fully implemented and USAID had not closed the recommendation. Therefore, we are not making a new recommendation at this time. However, we recommend the following for the remaining weaknesses:

***Recommendation 7:** We recommend that the chief information officer establish a process to monitor the operation of the automated script that disables accounts after 90 days of inactivity.*

***Recommendation 8:** We recommend that the chief information officer (a) identify system owners; (b) require them to verify their procedures for revoking system access accounts for separated and transferred employees and contractors are enforced, and (c) document their responses.*

4. USAID Needs to Implement a Process to Monitor for Unauthorized Software

NIST SP 800-53, Revision 4, privacy control CM-11, states the following regarding user installed software:

The organization:

* * *

- b. Enforces software installation policies through [Assignment: organization-defined methods]; and
- c. Monitors policy compliance at [Assignment: organization-defined frequency].

USAID ADS Chapter 545, Section 545.3.3.8 System and Services Acquisition, states "(19) SOs must enforce explicit rules governing the installation of software by users."

USAID had not documented and implemented a process to monitor for unauthorized software at an agency-defined frequency. Management specified that configuration settings were in place to prevent users from installing software on their laptops and workstations, therefore a process was not needed to monitor for unauthorized software at a defined frequency. However, this would not capture all unauthorized software that has already been installed.

¹⁶ Recommendation 13, *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-17-001-C, October 27, 2016).

Installing unauthorized software increases the risk of introducing viruses, and other malicious programs to USAID's systems potentially exposing the agency's information to unauthorized access. As a result, we recommend the following:

Recommendation 9: *We recommend that the chief information officer document and implement a procedure to check for unauthorized software at established intervals.*

5. USAID Needs to Strengthen Personnel Out-Processing Procedures

NIST SP 800-53, Revision 4, security control PS-4, states the following regarding personnel termination:

The organization, upon termination of individual employment:

- a. Disables information system access within [Assignment: organization-defined time period];
- b. Terminates/revokes any authenticators/credentials associated with the individual;
- c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
- d. Retrieves all security-related organizational information system-related property;
- e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
- f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

USAID ADS 451 Mandatory Reference, *Separation and Exit Clearance Process*, dated April 21, 2016, states:

- The AMS is responsible for providing the AID 451-1 form to the separating employee at least 10 business days in advance of departure along with the Employment Search and Post-Employment Guidance, the link to take the Exit Survey, and instructions on the Exit Interview. More information on the Exit Survey and the Exit Interview can be found in 451.3.5 and 451.3.6, respectively.
- After SEC's certification of the AID 451-1 form, the separating employee takes the form to the Office of Human Capital and Talent Management (HCTM) Records Center for filing and transmission to the Payroll Office for processing any final pay due to the employee.

Controls were not adequate to ensure USAID effectively managed separated employees. Specifically, we noted that five of the 25 sampled separated employees from a total population of 341, did not have an exit clearance form on file.

The Office of the CIO and system owners did not consistently receive exit forms from HCTM, Contracting Officer Representatives and Administrative Management Staff Officers, who are required to provide full exit notification and retrieval of USAID security-related property when employees and contractors leave the agency.

By not ensuring the employee separation process was completed properly, including the completion of all necessary documentation, collection of all organization property (badges, keys, keycards, etc.), and revocation of all employee access, USAID's security as well as information integrity may become compromised.

Although USAID documented procedures regarding the separation and exit clearance process, they did not fully implement the process. Because USAID officially closed the recommendations addressing this finding that were made in the fiscal year 2014,¹⁷ 2015,¹⁸ and 2016 FISMA audits;¹⁹ we are issuing the following new recommendation to correct this weakness:

Recommendation 10: *We recommend that the chief human capital officer document and implement a process to verify that all employees' exit clearance forms are completed and maintained in accordance with policy.*

6. USAID Needs to Monitor Remote Access Connections

NIST SP 800-53, Revision 4, security control AC-17, states the following regarding review and analysis of audit records.

The organization:

* * *

Control Enhancements:

(1) REMOTE ACCESS | AUTOMATED MONITORING / CONTROL

The information system monitors and controls remote access methods.

Although remote access activity was logged, management did not provide evidence that remote access connections were reviewed and analyzed. Management specified that the responsibility for monitoring remote access logs was previously under the purview of the engineering team. In June 2017, the responsibility was transferred to Information Technology Operations (ITO) and procedures to periodically review remote access logs had not been developed.

Without monitoring remote access logs, unauthorized individuals may gain system access and conduct malicious activities without detection. As a result, we recommend the following:

Recommendation 11: *We recommend that the chief information officer document and implement a procedure to review and analyze remote access connections.*

¹⁷ Recommendation 18, *Audit of USAID's Fiscal Year 2014 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-000-15-003-P, October 30, 2014).

¹⁸ Recommendation 2, *Audit of USAID's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002* (Audit Report No. A-000-15-010-P, September 25, 2015).

¹⁹ Recommendations 13 and 14, *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-17-001-C, October 27, 2016).

7. Information System Agreements Need to be Current

NIST SP 800-53, Revision 4, security control CA-3, states the following regarding system interconnection:

The organization:

- a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
- b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
- c. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].

Controls were not adequate to ensure USAID had current memorandums of understanding (MOU) and interconnection security agreements (ISA) covering the interconnection between one system and all entities with external connections. For example for one system tested, a documented agreement did not exist for the interconnection between this system and two external connections and the interconnection agreements had expired for two other external connections.

USAID did not have a process in place to ensure memorandums of understanding and interconnection security agreements were reviewed and monitored on a periodic basis. Management indicated that the memorandum of understanding and interconnection security agreements were being tracked, but had expired due to oversight.

Without a current agreement, there is an increased likelihood of one party not properly protecting information or reporting security incidents to appropriate personnel.

A recommendation addressing this finding was made in the fiscal year 2016 audit;²⁰ however, procedures were not fully implemented and USAID had not closed the recommendation. Therefore, we are not making a new recommendation at this time.

8. USAID Needs to Implement Role Based 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.

²⁰ Ibid. footnote 9.

In addition, ADS Chapter 545, states, “(3) USAID employees, staff, contractors, or others working on behalf of USAID with significant security responsibilities (e.g., ISSOs and SAs) must receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities. When access to an Information system is contractual the COR must ensure that contractors complete the appropriate specialized training and refresher courses.”

The FY 2015²¹ and 2016 audits²² reported that a role-based training program was not in place for personnel with significant information security responsibilities. USAID completed development of a role based training program in June of 2017; however, the training was not completed at the time of testing.

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. Personnel may be performing tasks without proper training, thus potentially increasing the risk that the agency’s information and information system could become compromised leading to unauthorized access, data loss, data manipulation and unavailability.

A recommendation addressing role-based training was made in the fiscal year 2015 audit;²³ however, procedures were not fully implemented and USAID had not closed the recommendation. Therefore, we are not making an additional recommendation at this time.

9. USAID Needs to Ensure Session Lock for Remote Access is Configured in Accordance with Agency Policy

NIST SP 800-53, Revision 4, security control AC-11, states the following regarding session lock:

The information system:

- a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and
- b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

USAID ADS Chapter 545, Section 545.3.6.6, Mobile Computing Devices, states, “(4) SOs must use a “time-out” function for remote access and Mobile Computing Devices requiring user re-authentication after fifteen (15) minutes of inactivity.”

²¹ *Audit of USAID’s Fiscal Year 2015 Compliance with the Federal Information Security Management Act Of 2002, as Amended* (Audit Report No. A-000-15-010-P), September 25, 2015).

²² *USAID has Implemented Controls in Support of FISMA, but Improvements are Needed* (Audit Report No. A-000-17-001-C, October 27, 2016).

²³ *Ibid.* footnote 8.

The remote access "Idle Timeout" setting was not configured in accordance with USAID policy. Management indicated that the setting was incorrectly set by the engineering team. The responsibility for configuring this setting was transferred to ITO in June 2017, and the setting was changed to be in compliance with agency policy. Since management remediated the issue upon notification, we are not making a recommendation at this time.

EVALUATION OF MANAGEMENT COMMENTS

In response to the draft report, the U.S. Agency for International Development (USAID) outlined its plans to address all 11 recommendations. USAID's comments and attachment Tab A of their response are included in their entirety in Appendix II.

Based on our evaluation of management comments, we acknowledge management decisions on all 11 recommendations for fiscal year 2017 and we agree with the final actions taken for recommendation 8.

In response to prior year Recommendation 17²⁴ - *Information System Agreements Need to be Current*, USAID management noted that procedures have been created to monitor and ensure that all connections to the authorized system have been formally approved and that the security state of the system is maintained per Interconnection Security Agreements (ISAs). In addition, USAID management noted that the CIO conducts weekly FISMA meetings to discuss the status of FISMA related issues such as prior year finding remediation status, and ongoing continuous monitoring activities including the status of expiring ATOs. As part of this meeting, a Cyber Security Assessment and Management (CSAM) "Systems Relationship Query" report is run to identify all existing MOUs and ISAs to determine the status of ATOs, and what follow-up actions are necessary to make sure the agreements are signed prior to expiration. However, as noted in Recommendation 17, for one system tested, a documented agreement did not exist for the interconnection between this system and two external connections and the interconnection agreements had expired for two other external connections. Though procedures and processes are in place, the process is not fully implemented.

In response to prior year Recommendation 13²⁵ - *USAID Needs to Implement Role Based Security Training*, USAID management noted that the finding was effectively closed by USAID Audit Performance and Compliance (APC) group on September 29, 2016 and is no longer an open recommendation as is being reported. However, as noted in Recommendation 13, USAID completed development of a role based training program in June of 2017; however, the training was not completed at the time of testing. As a result, the effectiveness of the program was not tested during the audit period.

²⁴ Ibid. footnote 9

²⁵ Ibid. footnote 8

SCOPE AND METHODOLOGY

Scope

We conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's (GAO) Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether USAID implemented certain security controls for selected information systems²⁶ in support of FISMA.

The audit included the testing of certain management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. We assessed USAID's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Physical and Environmental Protection
- Personnel Security
- Planning
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Communications Protection
- System and Services Acquisition

For this audit, we reviewed six (three internal and three external) out of the total population of 45 systems as of March 27, 2017. See Appendix II for a listing of selected controls. The audit also included an assessment of USAID's process for identifying and correcting/mitigating technical vulnerabilities. In addition, the audit included a follow up on prior audit recommendations²⁷ to determine if USAID made progress in implementing the recommended improvements concerning its information security program.

The audit fieldwork was performed at the USAID offices in Washington, D.C. and Arlington, VA from March 8, 2017, to August 24, 2017.

²⁶ See Appendix III for a list of systems and controls selected.

²⁷ Ibid. footnote 21 and 22.

Methodology

To determine if USAID's information security program met FISMA requirements, we conducted interviews with USAID officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. We also 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; and (5) change control documentation. Where appropriate, we compared documents, such as USAID's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

In addition, we completed a vulnerability assessment of one system and four missions out of the total population of 64, including a wireless assessment at two Agency headquarters locations and evaluated USAID's process for identifying and correcting/mitigating technical vulnerabilities. This included a review of USAID vulnerability scanning configurations and results and comparing them with independent network vulnerability scan results.

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

MANAGEMENT COMMENTS



September 27, 2017

MEMORANDUM

TO: Director IG/A/ITA, Mark Norman

FROM: M/CIO Deputy Chief Information Officer, Mark Johnson /s/
(On behalf of CIO- Jay Mahanand)

SUBJECT: Management Response to Audit of USAID's Fiscal Year 2017 Compliance with the Federal Information Security Management Act of 2002 (Audit Report No. A-000-XX-0XX-P, dated September XX 2017)

Thank you for the opportunity to respond to the draft audit report and audit recommendations as provided to M/CIO on September 20, 2017. This memorandum contains the management decisions for the recommendations provided by the OIG for the audit of USAID's Compliance with the Federal Information Security Management Act for Fiscal Year 2017.

The management decisions and proposed corrective actions are provided in Tab A of this memorandum. Documentation of HCTM's approval of the management response for recommendation 10 is provided in Tab H.

CC

HCTM Brenda Horne (/S/ 9/27/2017 Recommendation 10)

Tab A - Management Decisions

Recommendation 1: We recommend that the Chief Information Officer document and implement a process to track and remediate persistent vulnerabilities, or document acceptance of the associated risks.

Management Decision: M/CIO will document and implement a process to track and remediate persistent vulnerabilities, or document acceptance of the associated risks.

Target Date: 3/31/18

Recommendation 2: We recommend that the chief information officer document and implement a process to verify that vulnerability assessment tools are configured to detect vulnerabilities previously undiscovered by internal scans.

Management Decision: M/CIO will work with the vendor and IA CSIRT to document and implement a process to ensure timely detection of previously unfound vulnerabilities.

Target Date: 3/31/18

Recommendation 3: We recommend that the chief information officer develop and implement a documented process to migrate unsupported applications from their existing platform to vendor-supported platforms. The risk and approval, including adequate compensating controls, should be documented if an exception must be made until the unsupported software is migrated to vendor-supported platforms.

Management Decision: M/CIO is in the process of documenting a governance process to address unsupported applications and working with end users to either (1) remove the unsupported application (2) receive a waiver for the unsupported application to remain on the system or (3) upgrade the unsupported application.

Target Date: 3/31/18

Recommendation 4: We recommend that the chief information officer document and implement a process to verify Microsoft Windows systems comply with the U.S. Government Configuration Baseline and to grant and disseminate approved deviations from the baseline configuration settings.

Management Decision: M/CIO will document and implement a procedure to ensure Microsoft Windows systems are in compliance with the United States Government Configuration Baseline and document, approve, and disseminate approved deviations from the baseline.

Target Date: 9/30/18

Recommendation 5: We recommend that the chief information officer document and implement a plan to confirm all internal and external systems are currently authorized to operate.

Management Decision: M/CIO will document and implement a procedure to make sure all internal and external systems have a current authority to operate.

Target Date: 5/30/18

Recommendation 6: We recommend that the chief information officer document and implement a plan to annually assess system risks for all internal and external systems in accordance with agency policy.

Management Decision: M/CIO will document and implement a procedure to make sure an annual assessment for all systems is performed to assess system risks in accordance with agency policy.

Target Date: 3/31/18

Recommendation 7: We recommend that the chief information officer establish a process to monitor the operation of the automated script that disables accounts after 90 days of inactivity.

Management Decision: M/CIO will develop and implement a process to monitor the operation of the automated script for ensuring accounts are disabled after 90 days of inactivity.

Target Date: 3/31/18

Recommendation 8: We recommend that the chief information officer (a) identify system owners; (b) require them to verify that their procedures for revoking system access accounts for separated and transferred employees and contractors are enforced, and (c) document their responses.

Management Decision: M/CIO believes sufficient action has been taken to address this recommendation. The failure identified in the report is a result of system owners not being timely notified by HCTM and/or M/OAA of employee and contractor departures. M/CIO believes controls to revoke access at the system level works appropriately when these notifications are received. System owners are identified and documented within the Cyber Security Assessment and Management (CSAM) tool (Tab G). Furthermore, System Owners, along with their respective Information System Security Officers, are required as part of the documented USAID Continuous Monitoring Guide (Tab B) to assess select security control on an annual basis as part continuous monitoring activities, as well as assess all controls tri-annually as part of the USAID Security Assessment and

Authorization Process (Tab C), to validate that security controls are operating effectively. This includes account management controls for revoking system access. This verification is documented in CSAM and reported as part of system Security Assessment and Authorization activities (Tab D), which are reviewed and approved by the CIO as the Authorizing Official for all USAID systems.

Target Date: The Agency requests that this recommendation be closed upon issuance of the report based on the supporting documentation listed and included as attachments.

Recommendation 9: We recommend that the chief information officer document and implement a procedure to check for unauthorized software at established intervals.

Management Decision: M/CIO will document and implement a procedure to monitor for unauthorized software at a defined frequency.

Target Date: 8/30/18

Recommendation 10: We recommend that the chief human capital officer document and implement a process to verify that all employees' exit clearance forms are completed and maintained in accordance with policy.

Management Decision: The Office of Human Capital and Talent Management will document and implement a process to verify that all employees' exit clearance forms are completed and maintained in accordance with policy.

Target Date: 8/30/18

Recommendation 11: We recommend that the chief information officer document and implement a procedure to review and analyze remote access connections.

Management Decision: M/CIO will document and implement a procedure to review and analyze remote access connections.

Target Date: 8/30/18

Findings issued without Recommendation:**1. Information System Agreements Need to be Current**

Controls were not adequate to ensure USAID had current memorandums of understanding (MOU) and interconnection security agreements (ISA) covering the interconnection between one system and all entities with external connections. For example for one system tested, a documented agreement did not exist for the interconnection between this system and two external connections and the interconnection agreements had expired for two other external connections.

USAID did not have a process in place to ensure memorandums of understanding and interconnection security agreements were reviewed and monitored on a periodic basis. Management indicated that the memorandum of understanding and interconnection security agreements were being tracked, but had expired due to oversight.

Without a current agreement, there is an increased likelihood of one party not properly protecting information or reporting security incidents to appropriate personnel. A recommendation addressing this finding was made in the fiscal year 2016 audit; however, procedures were not fully implemented and USAID had not closed the recommendation. Therefore, we are not making a new recommendation at this time.

M/CIO Response: M/CIO believes appropriate action has been taken to address this recommendation and requests that it be closed upon issuance of the report. Specifically, M/CIO has documented and implemented the *USAID Continuous Monitoring Guide for Non-Cloud Systems* (Tab B), which describe policy and reporting requirements in support of continuous monitoring for USAID non-cloud systems. Additional objectives of the guide are to help ensure annual reauthorization of systems through the Chief Information Security Officer (CISO), Authorizing Officials (AOs), System Owners (SOs), Information System Security Officers (ISSOs), and/or designees; to document the Agency continuous monitoring process; to name roles and responsibilities; to generate required deliverables and artifacts; to help ensure compliance with policy guidance; to help systems gain an Authorization to Operate (ATO); and ultimately to help protect Agency assets and operations within the Agency RMF.

Specifically, section 6.4 of this document, entitled *Monitor Information System Connections*, outlines specific requirements for respective SOs to monitor system interconnections. In so doing, the SO must ensure that all connections to the authorized system have been formally approved and that the security state of the system is maintained per Interconnection Security Agreements (ISAs).

Furthermore, section 7.6, *Annual Requirements*, states that SOs must perform reviews and updates of their System Security Plans (SSPs). Section 11 of all USAID SSPs, System

Interconnections/Information Sharing, documents the respective system interconnections including the following information for each interconnection:

- Owning organization
- Interface Type
- Data Transfer Method
- Data Transfer Type
- Whether an agreement is on file and when it expires
- Classification of the system
- Contact information for the AO of the interfaced system

Finally, the CIO conducts weekly FISMA meetings to discuss the status of FISMA related issues (sample agenda provided in Tab E) such as prior year finding remediation status, and ongoing continuous monitoring activities including the status of expiring ATOs. As part of this meeting, a CSAM “*Systems Relationship Query*” (Tab F) report is run to identify all existing MOUs and ISAs to determine the status of ATOs, and what follow-up actions are necessary to make sure the agreements are signed prior to expiration. M/CIO believes the implementation of these procedures will ensure appropriate agreements with connected systems remain current and approved.

2. USAID Needs to Implement Role Based Security Training

The FY 2015 and 2016 audits reported that a role-based training program was not in place for personnel with significant information security responsibilities. USAID completed development of a role based training program in June of 2017; however, the training was not completed at the time of testing.

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. Personnel may be performing tasks without proper training, thus potentially increasing the risk that the agency’s information and information system could become compromised leading to unauthorized access, data loss, data manipulation and unavailability.

A recommendation addressing role-based training was made in the fiscal year 2015 audit; however, procedures were not fully implemented and USAID had not closed the recommendation. Therefore, we are not making an additional recommendation at this time.

M/CIO Response: M/CIO believes appropriate action has been taken to address this weakness and is requesting it be closed upon issuance. The finding referenced, is *Audit of USAID’s Fiscal Year 2015 Compliance with the Federal Information Security Management Act Of 2002, as Amended, Recommendation 13*. This finding was effectively closed by USAID APC on September 29, 2016 (Tab F), and is no longer an open recommendation as is being reported.

Summary of Controls Reviewed

The following table provides a summary of the controls selected for review for the FY 2017 audit. We did not review each control for each system. Additional controls were reviewed as a result of follow up testing for prior year recommendations.

Control No.	Control Name	# of Systems Reviewed
AC-1	Account Control Policies and Procedures	2
AC-2	Account Management	6
AC-3	Access Enforcement	4
AC-4	Information Flow Enforcement	3
AC-5	Separation of Duties	5
AC-6	Least Privilege	5
AC-8	System Use Notification	1
AC-11	Session Lock	3
AC-12	Session Termination	1
AC-17	Remote Access	1
AC-19	Access Control for Mobile Devices	1
AC-20	Use of External Information Systems	1
AT-1	Security Awareness & Training Policy and Procedures	1
AT-2	Security Awareness	1
AT-3	Security Training	1
AT-4	Security Training Records	1
CA-1	Security Assessment and Authorization Policies and Procedures	1
CA-2	Security Assessments	4
CA-3	System Interconnections	3
CA-5	Plan of Action and Milestones	5
CA-6	Security Accreditation	3
CA-7	Continuous Monitoring	1
CM-1	Configuration Management Policy & Procedures	1
CM-2	Baseline Configuration	4
CM-3	Configuration Change Control	4
CM-4	Security Impact Analysis	4
CM-5	Access Restrictions for Change	2
CM-6	Configuration Settings	3
CM-7	Least functionality	1
CM-8	Information System Component Inventory	1

Control No.	Control Name	# of Systems Reviewed
CM-10	Software Usage Restrictions	1
CM-11	User Installed Software	1
CP-1	Contingency Planning Policy & Procedures	2
CP-2	Contingency Plan	5
CP-3	Contingency Training	4
CP-4	Contingency Plan Testing and Exercises	4
CP-6	Alternate Storage Sites	1
CP-7	Alternate Processing Sites	2
CP-8	Telecommunication Services	1
CP-9	Information System Backup	3
CP-10	Information System Recovery & Reconstitution	4
IA-1	Identification & Authentication Policy and Procedures	1
IA-2	User Identification & Authentication (Organizational Users)	1
IA-3	Device Identification & Authentication	1
IA-4	Identifier Management	1
IA-5	Authentication Management	1
IR-1	Incident Response Policy & Procedures	1
IR-4	Incident Handling	1
IR-5	Incident Monitoring	1
IR-6	Incident Reporting	1
IR-8	Incident Response Plan	1
MA-2	Controlled Maintenance	1
MA-5	Maintenance Personnel	1
MA-6	Timely Maintenance	1
PE-2	Physical Access Authorizations	1
PE-3	Physical Access Control	1
PL-2	System Security Plan	3
PL-4	Rules of Behavior	2
PS-4	Personnel Termination	1
PS-5	Personnel Transfer	1
PS-6	Access Agreements	1
RA-1	Risk Assessment Policy and Procedures	1
RA-2	Security Categorization	1
RA-3	Risk Assessment	4
RA-5	Vulnerability Scanning	3
SA-3	System Development Life Cycle	4

Control No.	Control Name	# of Systems Reviewed
SA-4	Acquisitions Process	2
SA-5	Information System Documentation	4
SA-9	External Information System Services	3
SC-7	Boundary Protection	1
SC-8	Transmission Confidentiality and Integrity	2
SI-2	Flaw remediation	2
PM-1	Information Security Program Plan	1
PM-3	Information Security Resources	1
PM-4	Plan Of Action And Milestones Process	1
PM-5	Information System Inventory	1
PM-6	Information Security Measures Of Performance	1
PM-7	Enterprise Architecture	1
PM-9	Risk Management Strategy	1
PM-10	Security Authorization Process	1
PM-14	Testing, Training, and Monitoring	1
AR-5	Privacy Awareness and Training	1