U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Special Report

Fiscal Year 2010 Federal Information Security Management Act Report

Status of EPA's Computer Security Program

Report No. 11-P-0017

November 16, 2010

Abbreviations

AC	Access Controls
CD	Compact Disc
CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IG	Inspector General
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plans of Actions & Milestones
TT&E	Training, Testing, and Exercises
US-CERT	United States Computer Emergency Readiness Team

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

November 16, 2010

MEMORANDUM

SUBJECT: Fiscal Year 2010 Federal Information Security Management Act Report: Status of EPA's Computer Security Program
Report No. 11-P-0017

FROM: Arthur A. Elkins, Jr.
Inspector General

TO: Lisa P. Jackson
Administrator

Attached is the Office of Inspector General's (OIG's) Fiscal Year 2010 Federal Information Security Management Act (FISMA) Reporting Template, as prescribed by the Office of Management and Budget (OMB). The OIG and its contractor, Williams, Adley and Company, LLP (Williams Adley), jointly performed this review in accordance with generally accepted government auditing standards. These standards require the team to plan and perform the review to obtain sufficient and appropriate evidence to provide a reasonable basis for the findings and conclusions based on the objectives of the review.

We believe the evidence obtained provides a reasonable basis for our findings and conclusions, and in all material respects, meets the FISMA reporting requirements prescribed by OMB. In accordance with OMB reporting instructions, I am forwarding this report to you for submission, along with the Agency's required information, to the Director of OMB.

The audit work performed during the FISMA review disclosed a significant deficiency that requires EPA to take immediate or near-immediate corrective action in establishing and maintaining an account and identity management program for user accounts that reside on the Agency's network. While we found the Agency took steps to identify inactive network accounts, EPA offices do not take appropriate action to timely disable or terminate the accounts.

In addition, audit work during Fiscal Year 2010 noted significant weaknesses with several aspects of EPA's information security program. Appendix A summarizes the results from these audit reports.

The estimated cost for performing this audit, which includes contract costs and OIG contract management oversight, is $463,269.

Inspector General

Section Report

2010

Annual FISMA Report

Environmental Protection Agency

Section 1: Status of Certification and Accreditation Program

1. Selected response is:

a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.

2. Establishment of accreditation boundaries for agency information systems.

3. Categorizes information systems.

4. Applies applicable minimum baseline security controls.

5. Assesses risks and tailors security control baseline for each system.

6. Assessment of the management, operational, and technical security controls in the information system.

7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.

8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.

Section 2: Status of Security Configuration Management

2. Selected response is:

a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures for configuration management.

2. Standard baseline configurations.

3. Scanning for compliance and vulnerabilities with baseline configurations.

4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented.

5. Documented proposed or actual changes to the configuration settings.

6. Process for the timely and secure installation of software patches.

3. Identify baselines reviewed:

Section 2: Status of Security Configuration Management

Operating System
Microsoft Windows Server 2003
Microsoft Windows XP Professional

Section 3: Status of Incident Response & Reporting Program

4. Selected response is:

a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. **Documented policies and procedures for responding and reporting to incidents.**
2. **Comprehensive analysis, validation and documentation of incidents.**
3. **When applicable, reports to US-CERT within established timeframes.**
4. **When applicable, reports to law enforcement within established timeframes.**
5. **Responds to and resolves incidents in a timely manner to minimize further damage.**

Section 4: Status of Security Training Program

5. Selected response is:

a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. **Documented policies and procedures for security awareness training.**
2. **Documented policies and procedures for specialized training for users with significant information security responsibilities.**
3. **Appropriate training content based on the organization and roles.**
4. **Identification and tracking of all employees with login privileges that need security awareness training.**
5. **Identification and tracking of employees without login privileges that require security awareness training.**
6. **Identification and tracking of all employees with significant information security responsibilities that require specialized training.**

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

6. Selected response is:

a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures for managing all known IT security weaknesses.
2. Tracks, prioritizes and remediates weaknesses.
3. Ensures remediation plans are effective for correcting weaknesses.
4. Establishes and adheres to reasonable remediation dates.
5. Ensures adequate resources are provided for correcting weaknesses.
6. Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POAM activities at least quarterly.

Section 6: Status of Remote Access Program

7. Selected response is:

a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.
2. Protects against unauthorized connections or subversion of authorized connections.
3. Users are uniquely identified and authenticated for all access.
4. If applicable, multi-factor authentication is required for remote access.
5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.
6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.
7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.

Section 7: Status of Account and Identity Management Program

8. Selected response is:

b. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.

8a. Areas for Improvement:

8a(1). Account management policy is not fully developed.

Section 7: Status of Account and Identity Management Program

No

8a(2). Account management procedures are not fully developed, sufficiently detailed or consistently implemented.

No

8a(3). Active Directory is not properly implemented (NIST 800-53, AC-2).

No

8a(4). Other Non-Microsoft account management software is not properly implemented(NIST 800-53, AC-2).

No

8a(5). Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).

No

8a(6). Accounts are not properly issued to new users (NIST 800-53, AC-2).

No

8a(7). Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).

Yes

Comments: The FISMA review disclosed a significant deficiency that requires EPA to take immediate or near-immediate corrective action in establishing and maintaining an account and identity management program for user accounts that reside on the Agency's network. While we found the Agency took steps to identify inactive network accounts, EPA offices do not take appropriate action to timely disable or terminate the accounts.

8a(8). Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).

No

8a(9). Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).

No

8a(10). Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).

No

8a(11). Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).

No

8a(12). Network devices are not properly authenticated (NIST 800-53, IA-3).

No

Section 7: Status of Account and Identity Management Program

8a(13). Other

No

Section 8: Status of Continuous Monitoring Program

9. Selected response is:

a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures for continuous monitoring.

2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc.

3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.

4. Provides system authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions.

Section 9: Status of Contingency Planning Program

10. Selected response is:

a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.

2. The agency has performed an overall Business Impact Assessment.

3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

4. Testing of system specific contingency plans.

5. The documented business continuity and disaster recovery plans are ready for implementation.

6. Development of training, testing, and exercises (TT&E) approaches.

7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

Section 10: Status of Agency Program to Oversee Contractor Systems

Section 10: Status of Agency Program to Oversee Contractor Systems

11. Selected response is:

a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines.

2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities.

3. The inventory identifies interfaces between these systems and Agency-operated systems.

4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that is owns and operates.

5. The inventory, including interfaces, is updated at least annually.

6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.

Appendix A

Summary of Significant Fiscal Year 2010 Security Control Audits

During Fiscal Year 2010, the U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) published the following audit reports of EPA's information technology security program and information systems. The following summarizes key findings.

1. ECHO Data Quality Audit - Phase 2 Results: EPA Could Achieve Data Quality Rate With Additional Improvements, Report No. 10-P-0230, September 22, 2010

OIG contractors, KPMG, LLP, found that EPA mandates that data elements reported to the public through the Enforcement Compliance and History Online (ECHO) website have a 95 percent accuracy rate. KPMG found a 91.5 percent data accuracy rate for key data elements entered into two primary ECHO source systems: the legacy Permit Compliance System and the newer Integrated Compliance Information System – National Pollutant Discharge Elimination System. Although the 91.5 percent data quality rate is close to EPA's goal, EPA and the state environmental offices could take additional steps to increase the quality of data reported through the ECHO website. The Agency generally agreed with the report findings.

2. Steps Needed to Prevent Prior Control Weaknesses From Affecting New Acquisition System, Report No. 10-P-0160, June 28, 2010

OIG contractors, Williams Adley & Company, LLC, found that stronger system controls over the Integrated Contracts Management System (ICMS) need to be addressed prior to transitioning to the new EPA Acquisition System (EAS). Williams, Adley & Company, LLP, noted that:

- System reporting does not always accurately associate a procurement action with the correct user who initiated the action.
- ICMS does not have an audit log to capture and allow monitoring of security events.
- No formal ICMS user training exists.
- The ICMS Continuity of Operations Plan and system backup procedures are not compliant with federal requirements.
- ICMS generates procurement documents in a format such that changes to the procurement documents can be made outside of the ICMS processing environment.

While it may not be practical for EPA to address these weaknesses within ICMS, EPA should take proactive steps to strengthen its system controls prior to transitioning to the EAS so that similar weaknesses do not exist in EAS.

3. Improvements Needed in Key EPA Information System Security Practices, Report No. 10-P-0146, June 15, 2010

OIG contractors, Williams Adley & Company, LLC, found that EPA program offices lacked evidence that they planned and executed tests of information system security controls as required by federal requirements. In addition, Williams Adley found that contingency plans developed and maintained by program offices were not current and accurate, and the certification and accreditation process and review of security plans needed improvements. EPA also had two authoritative system inventories that did not reconcile. Finally, EPA had contractor-owned and -operated systems in operation without proper oversight monitoring. Agency officials did not provide comments to the draft audit report and indicated that they will provide a response to the final report.

4. Improved Data Integrity Needed for the Integrated Contracts Management System, Report No. 10-P-0144, June 14, 2010

OIG contractors, Williams Adley & Company, LLP, found that EPA needs to strengthen Integrated Contracts Management System (ICMS) data integrity controls to increase the reliability of the data for management reporting. In particular, ICMS data contain exceptions to data quality rules defined in the ICMS data dictionary and Office of Acquisition Management (OAM)-defined system checks. ICMS data also contain anomalies that cast suspicion over the validity of processed transactions. These anomalies include transactions processed on nonstandard workdays and dollar values that are unusually high. Furthermore, discrepancies noted between OAM-defined system edit and validation checks and the ICMS data dictionary call into question what actual information should be entered into the ICMS for certain fields. The above conditions are caused by a breakdown in controlling data entry or in maintaining data and associated system documentation. The Agency generally agreed with the findings and recommendations.

5. Plans to Migrate Data to the New EPA Acquisition System Need Improvement, Report No. 10-P-0071, February 24, 2010

OIG contractors, Williams, Adley & Company, LLC, found that EPA's plans for migrating data from the Integrated Contracts Management System (ICMS) to EPA's Acquisition System (EAS) lack sufficient incorporation of data integrity and quality checks to ensure the complete and accurate transfer of procurement data. In particular, verification of overall data accuracy relies heavily on contracting officers to review their own contract data in EAS after it has been migrated from ICMS. However, EPA does not require that contracting officers attend data migration training. In addition, plans to migrate closed contracts do not require verification of the accuracy and completeness of that data, which will be utilized for historic reporting purposes in EAS. While EAS data validation and edit checks will enforce integrity constraints over user-entered data, proper data migration controls are paramount to ensuring that the acquisition data transfer accurately and completely from ICMS to EAS. The Agency generally agreed with the findings and recommendations.

6. EPA Needs to Improve Physical Security at Its Offices in Las Vegas, Nevada, Report No. 10-P-0059, February 3, 2010

EPA needs to improve physical security at its Las Vegas facilities. The Las Vegas Finance Center's (LVFC's) server room and other key areas are susceptible to unauthorized access by personnel not a part of LVFC. The LVFC areas are protected by an access control system, but the system operator, the Office of Research and Development (ORD)-does not administer the system in a manner that allows LVFC to monitor access to its area. As a result, the ORD granted personnel access to sensitive LVFC areas without proper authorization. EPA agreed with the findings and recommendations.

7. Self-reported Data Unreliable for Assessing EPA's Computer Security Program, Report No. 10-P-0058, February 2, 2010

The oversight and monitoring procedures for the Automated System Security Evaluation and Remediation Tracking (ASSERT) system provide limited assurance the data are reliable for assessing EPA's computer security program. As a result:

- Unsubstantiated responses for self-reported information contribute to data quality problems.
- Limited independent reviews and lack of follow-up inhibit EPA's ability to identify and correct data inaccuracies.
- Independent reviews lack coordination with certification and accreditation activities.
- Information security personnel believe they need more training on how to assess security controls and feel pressure to answer system security questions in a positive manner.
- Limited internal reporting on required security controls and missing information in security plans inhibit external reporting.

Further, incomplete security documentation raises concerns as to whether the ASSERT application contractor is meeting federal requirements. The Agency agreed with all of our findings and recommendations.

8. Improved Security Planning Needed for the Customer Technology Solutions Project, Report No. 10-P-0028, November 16, 2009

EPA lacks a process to routinely test Customer Technology Solution (CTS) equipment for known vulnerabilities and to correct identified threats. Furthermore, EPA placed CTS equipment into production without fully assessing the risk the equipment poses to the Agency's network and authorizing the equipment for operations. The Office of Management and Budget requires federal agencies to create a security plan for each general support system and ensure the plan complies with guidance issued by the National Institute of Standards and Technology. Both vulnerability management and the preparation of critical security documents, such as the Security Plan and the Authorization to Operate, are paramount to fulfilling this requirement. These weaknesses exist because EPA undertook an aggressive schedule to install over 11,500 computers at 18 locations across the United States. As

problems occurred during installation, management focused its attention on addressing these issues in order to meet the deployment schedule milestone.

9. As part of the Fiscal Year 2010 FISMA Audit, the following series of network vulnerability reports were issued to EPA's offices to address high-risk and medium-risk vulnerabilities:

- Results of Technical Network Vulnerability Assessment: EPA's Andrew W. Breidenbach Environmental Research Center, Report No. 10-P-0210, September 7, 2010
- Results of Technical Network Vulnerability Assessment: EPA's Erlanger Building, Report No. 10-P-0211, September 7, 2010
- Results of Technical Network Vulnerability Assessment: EPA's Ronald Reagan Building, Report No. 10-P-0212, September 7, 2010
- Results of Technical Network Vulnerability Assessment: EPA's Region 4, Report No. 10-P-0213, September 7, 2010

The OIG met with EPA information security personnel to discuss the findings. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network.

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Director, Office of Technology Operations and Planning, Office of Environmental Information
Senior Agency Information Security Officer, Office of Environmental Information
Director, Technology and Information Security Staff, Office of Environmental Information
General Counsel
Agency Followup Official (the CFO)
Agency Followup Coordinator
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for External Affairs and Environmental Information