U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Fiscal Year 2011 Federal Information Security Management Act Report

Status of EPA’s Computer Security Program

Report No. 12-P-0062 **November 9, 2011**

Report Contributors:

Rudolph M. Brevard
Cheryl Reid
Scott Sammons
Christina Nelson
Kyle Denning

Abbreviations

APT	Advanced Persistent Threat
BIA	Business Impact Analysis
CA	Certification, Accreditation, and Security Assessments
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
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PM	Program Management
POA&M	Plan of Action & Milestones
RCRAInfo	Resource Conservation and Recovery Act Information System
SP	Special Publication
TT&E	Training, Testing, and Exercises
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline

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

THE INSPECTOR GENERAL

November 9, 2011

MEMORANDUM

SUBJECT: Fiscal Year 2011 Federal Information Security Management Act Report:
Status of EPA's Computer Security Program
Report No. 12-P-0062

FROM: Arthur A. Elkins, Jr.
Inspector General

Arthur A. Elkins

TO: Lisa P. Jackson
Administrator

Attached is the Office of Inspector General's (OIG's) Fiscal Year 2011 Federal Information Security Management Act (FISMA) Reporting Template, as prescribed by the Office of Management and Budget (OMB). We 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 that the Agency needs to make significant improvements in the following programs: (1) Risk Management, (2) Plans of Action & Milestones, and (3) Continuous Monitoring Management.

In addition, audit work during fiscal year 2011 noted significant weaknesses with several aspects of EPA's information security program. Appendix A summarizes the results from these audit reports.

Inspector General

Section Report

2011

Annual FISMA Report

Environmental Protection Agency

Section 1: Risk Management

1.b. **The Agency has established and is maintaining a risk management program. However, the Agency needs to make significant improvements as noted below.**

Comments: We limited our review to evaluating whether EPA fully developed Risk Management policies and procedures compliant with NIST SP 800-37. While EPA developed Risk Assessment guidance, the Agency had not fully developed a Risk Management Framework consistent with the latest NIST guidance. As such, we did not evaluate all of the Risk Management areas within this section.

1.b(1). **Risk Management policy is not fully developed.**

Yes

1.b(2). **Risk Management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53).**

Yes

1.b(3). **Risk Management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).**

No

Comments: We did not evaluate this area.

1.b(4). **A Comprehensive governance structure and Agency-wide risk management strategy has not been fully developed in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).**

No

Comments: We did not evaluate this area.

1.b(5). **Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53).**

No

Comments: We did not evaluate this area.

1.b(6). **Information systems are not properly categorized (FIPS 199/SP 800-60).**

No

1.b(7). **Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS 200/SP 800-53).**

No

1.b(8). **Risk assessments are not conducted in accordance with government policies (SP 800-30).**

No

Comments: We did not evaluate this area.

1.b(9). **Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53).**

No

1.b(10). **The communication of information system specific risks, mission/business specific risks and organizational level (strategic) risks to appropriate levels of the organization is not in accordance with government policies.**

No

Comments: We did not evaluate this area.

1.b(11). **The process to assess security control effectiveness is not in accordance with government policies (SP800-53A).**

No

1.b(12). **The process to determine risk to Agency operations, Agency assets, or individuals, or to authorize information systems to operate is not in accordance with government policies (SP 800-37).**

No

Comments: We did not evaluate this area.

1.b(13). **The process to continuously monitor changes to information systems that may necessitate reassessment of control effectiveness is not in accordance with government policies (SP 800-37).**

No

Comments: We did not evaluate this area.

1.b(14). **Security plan is not in accordance with government policies (SP 800-18, SP 800-37).**

No

Comments: We did not evaluate this area.

1.b(15). **Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37).**

No

Comments: We did not evaluate this area.

1.b(16). **Accreditation boundaries for Agency information systems are not defined in accordance with government policies.**

Section 1: Risk Management

No

Comments: We did not evaluate this area.

1.b(17). **Other**

No

Section 2: Configuration Management

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

2.a(1). **Documented policies and procedures for configuration management.**

Yes

2.a(2). **Standard baseline configurations defined.**

Yes

2.a(3). **Assessing for compliance with baseline configurations.**

Yes

2.a(4). **Process for timely, as specified in Agency policy or standards, remediation of scan result deviations.**

Yes

2.a(5). **For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.**

Yes

2.a(6). **Documented proposed or actual changes to hardware and software configurations.**

Yes

2.a(7). **Process for timely and secure installation of software patches.**

Yes

Section 3: Incident Response and Reporting

3a. **The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA**

Section 3: Incident Response and Reporting

requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

3a(1). **Documented policies and procedures for detecting, responding to and reporting incidents.**

Yes

3a(2). **Comprehensive analysis, validation and documentation of incidents.**

Yes

3a(3). **When applicable, reports to US-CERT within established timeframes.**

Yes

3a(4). **When applicable, reports to law enforcement within established timeframes.**

Yes

3a(5). **Responds to and resolves incidents in a timely manner, as specified in Agency policy or standards, to minimize further damage.**

Yes

3a(6). **Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.**

Yes

3a(7). **Is capable of correlating incidents.**

Yes

Comments: We are reviewing this area in a separate audit. We will issue our results in the final report during the third quarter of FY 2012.

Section 4: Security Training

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

4.a(1). **Documented policies and procedures for security awareness training.**

Yes

Section 4: Security Training

4.a(2). **Documented policies and procedures for specialized training for users with significant information security responsibilities.**

Yes

4.a(3). **Security training content based on the organization and roles, as specified in Agency policy or standards.**

Yes

4.a(4). **Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Agency users) with access privileges that require security awareness training.**

Yes

4.a(5). **Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Agency users) with significant information security responsibilities that require specialized training.**

Yes

Section 5: POA&M

5.b. **The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.**

5.b(1). **POA&M Policy is not fully developed.**

No

5.b(2). **POA&M procedures are not fully developed and sufficiently detailed.**

No

5.b(3). **POA&M procedures are not consistently implemented in accordance with government policies.**

No

5.b(4). **POA&Ms do not include security weaknesses discovered during assessments of security controls and requiring remediation. (OMB M-04-25).**

Yes

Comments: While EPA creates POA&Ms during annual self-assessments, the Agency does not consistently create POA&Ms for security weaknesses discovered during internal reviews.

5.b(5). **Remediation actions do not sufficiently address weaknesses in accordance with government policies (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).**

Section 5: POA&M

No

5.b(6). **Source of security weaknesses are not tracked (OMB M-04-25).**

No

5.b(7). **Security weaknesses are not appropriately prioritized (OMB M-04-25).**

No

5.b(8). **Milestone dates are not adhered to. (OMB M-04-25).**

No

5.b(9). **Initial target remediation dates are frequently missed (OMB M-04-25).**

Yes

Comments: 20% of EPA's FY 2011 POA&Ms missed the initial target remediation date by 30 or more days.

5.b(10). **POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).**

No

5.b(11). **Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).**

No

5.b(12). **Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).**

No

5.b(13). **Other**

No

Section 6: Remote Access Management

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

6.a(1). **Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.**

Yes

Section 6: Remote Access Management

6.a(2). **Protects against unauthorized connections or subversion of authorized connections.**

Yes

6.a(3). **Users are uniquely identified and authenticated for all access.**

Yes

6.a(4). **If applicable, multi-factor authentication is required for remote access.**

Yes

6.a(5). **Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.**

Yes

6.a(6). **Defines and implements encryption requirements for information transmitted across public networks.**

Yes

6.a(7). **Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required.**

Yes

Section 7: Identity and Access Management

7.a. **The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**

Comments: We did not evaluate this section because we are reviewing this area in a separate audit. We will issue our results in the final report during the second quarter of FY 2012.

7.a(1). **Documented policies and procedures for account and identity management.**

Yes

7.a(2). **Identifies all users, including federal employees, contractors, and others who access Agency systems.**

Yes

7.a(3). **Identifies when special access requirements (e.g., multi-factor authentication) are necessary.**

Section 7: Identity and Access Management

Yes

7.a(4). If multi-factor authentication is in use, it is linked to the Agency's PIV program where appropriate.

Yes

7.a(5). Ensures that the users are granted access based on needs and separation of duties principles.

Yes

7.a(6). Identifies devices that are attached to the network and distinguishes these devices from users.

Yes

7.a(7). Ensures that accounts are terminated or deactivated once access is no longer required.

Yes

7.a(8). Identifies and controls use of shared accounts.

Yes

Section 8: Continuous Monitoring Management

8.b. The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.

8.b(1). Continuous monitoring policy is not fully developed (NIST 800-53: CA-7).

No

8.b(2). Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7).

Yes

8.b(3). Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev 1, Appendix G).

No

Comments: We did not evaluate this area.

8.b(4). Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev 1, Appendix G).

Yes

8.b(5). Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53,

Section 8: Continuous Monitoring Management

NIST 800-53A).

No

8.b(6). The following were not provided to the authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).

No

8.b(7). Other

No

Section 9: Contingency Planning

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

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

Yes

9.a(2). The Agency has performed an overall Business Impact Analysis (BIA).

Yes

9.a(3). Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

Yes

9.a(4). Testing of system specific contingency plans.

Yes

9.a(5). The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.

Yes

9.a(6). Development of test, training, and exercise (TT&E) programs.

Yes

9.a(7). Performance of regular ongoing testing or exercising of business continuity/disaste ine effectiveness

Section 9: Contingency Planning

and to maintain current plans.

Yes

Section 10: Contractor Systems

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

10.a(1). Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

Yes

10.a(2). The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Agency guidelines.

Yes

10.a(3). A complete inventory of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

Yes

10.a(4). The inventory identifies interfaces between these systems and Agency-operated systems.

Yes

10.a(5). The Agency requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.a(6). The inventory of contractor systems is updated at least annually.

Yes

10.a(7). Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Yes

Section 11: Security Capital Planning

11.a. The Agency has established and maintains a security capital planning and investment program for information security. Although

Section 11: Security Capital Planning

improvement opportunities may have been identified by the OIG, the program includes the following attributes:

11.a(1). **Documented policies and procedures to address information security in the capital planning and investment control process.**

Yes

11.a(2). **Includes information security requirements as part of the capital planning and investment process.**

Yes

11.a(3). **Establishes a discrete line item for information security in organizational programming and documentation.**

Yes

11.a(4). **Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.**

Yes

11.a(5). **Ensures that information security resources are available for expenditure as planned.**

Yes

Appendix A

Summary of Significant Fiscal Year 2011 Security Control Audits

During fiscal year 2011, the EPA OIG published a number of audit reports on EPA's information technology security program and information systems. The following summarizes key findings:

1. ***Region 9 Technical and Computer Room Security Vulnerabilities Increase Risk to EPA's Network*, Report No. 11-P-0725, September 30, 2011**

   The OIG's physical and environmental control review of the Region 9 computer room found that sufficient protections were not in place to safeguard critical information technology assets and associated data from the risk of damage and/or loss.

2. ***EPA Has Taken Steps to Address Cyber Threats but Key Actions Remain Incomplete*, Report No. 11-P-0277, June 23, 2011**

   In association with an OIG investigation of Advanced Persistent Threats (APTs), the Agency reported that over 7,800 of its systems had communicated with known hostile Internet protocol addresses. These Agency systems potentially could have been compromised by APTs due to these communications. We issued previous reports and made recommendations that could help the Agency strengthen cyber security practices for combating APTs. However, some of those recommendations remain unimplemented, and we continue to find and report on similar weaknesses at other EPA locations. The Agency generally agreed with all the recommendations.

3. ***Improvements Needed in EPA's Network Traffic Management Practices*, Report No. 11-P-0159, March 14, 2011**

   The Office of Environmental Information (OEI) does not have consistent, repeatable intrusion detection system monitoring practices in place, which inhibits EPA's ability to monitor unusual network activity and thus protect Agency systems and associated data. OEI has not documented a methodology to aid in making decisions about potentially unusual network traffic and does not consistently conduct management oversight of contractor performance and reporting. In addition, key federally required security documents for EPA's Wide Area Network were not complete or accurate. The Agency agreed with our recommendations.

4. ***EPA Could Improve RCRAInfo Data Quality and System Development*, Report No. 11-P-0096, February 7, 2011**

   Resource Conservation and Recovery Act Information System (RCRAInfo) data that track hazardous waste handlers and the shipment and receipt of hazardous waste contain errors and are missing source documentation. These conditions call into question the quality and reliability of data within the RCRAInfo system, as well as any resulting reporting. RCRAInfo system owners did not follow the prescribed System Life Cycle Management testing procedures to test and validate the updated software and updated system. Further, field work found instances of test data comingled with production data. Overall, the above conditions were caused by not having specific data quality procedures for RCRAInfo that align with the Agency's data quality policy, not following the System Life Cycle Management procedures for system development, and not adequately communicating with the states regarding the RCRAInfo test environment. As required by the EPA quality policy, EPA organizations must document and implement a quality program for environmental data that are intended for external distribution.

5. *Improvements Needed in EPA's Efforts to Replace Its Core Financial System*, Report No. 11-P-0019, November 29, 2010

The Office of the Chief Financial Officer's (OCFO's) management control processes do not ensure compliance with EPA's Systems Life Cycle Management policies and procedures. EPA's system development policies and procedures identify specific activities and documents required during a system development project. However, OCFO's internal control environment does not enforce these policies and procedures. OCFO proceeded with the design subphase of the system project without obtaining executive management approval of the updated system requirements or developing and obtaining the required approval of test plans to ensure the system will meet Agency needs. Further, OCFO did not predetermine the acceptable product acceptance test script failure percentages to be used as the basis for management's go/no-go decision to proceed with using the evaluated product. The Agency agreed with all recommendations.

6. Technical Vulnerability Assessments

As part of the fiscal year 2011 FISMA audit, the OIG issued a series of network vulnerability reports to EPA offices to address high-risk and medium-risk vulnerabilities. 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. The first report listed below also appears as number 1 above, because it reported on our review of Region 9's physical and environmental controls as well as the results of our technical vulnerability assessment.

- *Region 9 Technical and Computer Room Security Vulnerabilities Increase Risk to EPA's Network*, Report No. 11-P-0725, September 30, 2011
- *Results of Technical Vulnerability Assessment: EPA's Directory Service System Authentication and Authorization Servers*, Report No. 11-P-0597, September 9, 2011
- *Results of Technical Network Vulnerability Assessment: EPA's National Health & Environment Effect Research Laboratory, Western Ecology Division*, Report No. 11-P-0429, August 3, 2011

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
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for External Affairs and Environmental Information
Audit Follow-Up Coordinator, Office of Environmental Information