U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Information Technology

Cybersecurity Act of 2015 Report: EPA's Policies and Procedures to Protect Systems With Personally Identifiable Information

Report No. 16-P-0259 **August 10, 2016**

REDACTED VERSION FOR PUBLIC RELEASE

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Nancy Dao
Peter Dragon
Nii-Lantei Lamptey
Christina Nelson

Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
NIST	National Institute of Standards and Technology
OASIS	Office of Administration Services Information System
OEI	Office of Environmental Information
OIG	Office of Inspector General
PII	Personally Identifiable Information
SAISO	Senior Agency Information Security Officer
SCORPIOS	Superfund Cost Recovery Package Imaging Online System

Cover image: EPA OIG image alluding to security.

Are you aware of fraud, waste or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

16-P-0259
August 10, 2016

At a Glance

Why We Did This Review

The Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA) conducted this audit to determine to what extent the EPA implemented information system security policies and procedures to protect agency systems that provide access to national security or Personally Identifiable Information (PII), as outlined in Section 406 of the Cybersecurity Act of 2015.

This report addresses the following EPA goal or cross-agency strategy:

- *Embracing EPA as a high-performing organization.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

Cybersecurity Act of 2015 Report: EPA's Policies and Procedures to Protect Systems With Personally Identifiable Information

What We Found

Section 406 of the Cybersecurity Act of 2015 calls for Inspectors General of agencies with covered systems to report on several aspects of the covered systems' information system security controls. The term "covered system" means a national security system as defined in 40 U.S.C. § 11103 or a federal computer system that provides access to PII.

The EPA has 30 systems that contain sensitive PII. Safeguarding information and preventing system breaches are essential for ensuring the EPA retains the trust of the American public.

The EPA has 30 covered systems that contain sensitive PII covered by provisions of the act. Of the 30 covered systems, two were sampled for our audit. Although the EPA has 30 systems that include sensitive PII, the EPA does not own any systems that include national security information.

The act requires Inspectors General to report on the areas identified in the bullets below. We provided information in the following eight areas based on the requirements outlined in the act for the EPA's covered systems.

- Description of logical access policies and practices.
- Description of the logical access controls and multifactor authentication used to govern privileged users access.
- Reasons for not using logical access controls and multifactor authentication if applicable.
- Policies and procedures used to conduct inventories of software and licenses.
- Capabilities utilized to monitor and detect exfiltration and other threats.
- Description of how monitoring and detecting capabilities are utilized.
- Reasons why monitoring and detecting capabilities are not used if applicable.
- Description of policies and procedures used to ensure entities and contractors providing services to the EPA are implementing the information security management practices identified in the act.

We issued a draft report containing our conclusions and briefed EPA representatives on the audit results. The EPA agreed with our results and emailed its responses, which were evaluated and incorporated into this report.

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.

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

THE INSPECTOR GENERAL

August 10, 2016

MEMORANDUM

SUBJECT: Cybersecurity Act of 2015 Report: EPA's Policies and Procedures to Protect Systems With Personally Identifiable Information
Report No. 16-P-0259

FROM: Arthur A. Elkins Jr.

TO: Ann Dunkin, Chief Information Officer
Office of Environmental Information

Donna Vizian, Acting Assistant Administrator
Office of Administration and Resources Management

David Bloom, Deputy Chief Financial Officer

This is our audit of the Cybersecurity Act of 2015 report as outlined by Section 406 of the act. The project number for this audit was OA-FY16-0126. We believe the evidence obtained provides a reasonable basis for our findings and conclusions and, in all material respects, meets the reporting requirements prescribed by Section 406 of the act.

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.

You are not required to provide a written response to this final report. In accordance with Section 406 of the act, we are forwarding the full version of this report to the appropriate committees of Congress.

Table of Contents

Appendix

Purpose

The Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA) performed this audit to determine to what extent the EPA implemented information system security policies and procedures to protect agency systems that provide access to national security or Personally Identifiable Information (PII), as outlined in Section 406 of the Cybersecurity Act of 2015.[1]

Background

Section 406 of the Cybersecurity Act requires an agency's Inspector General to submit to the appropriate congressional committees a report providing specific information collected from the agency regarding the protection of covered systems.

A covered system is a national security system as defined in 40 U.S.C. § 11103 or a federal computer system that provides access to PII.

As of January 6, 2015, the EPA had 30 agency systems that contained sensitive PII. The EPA does not own any systems that contain national security information, and none are reported in the agency's official system inventory.

Responsible Offices

The Office of Environmental Information (OEI) leads the EPA's information management and information technology programs, to provide the information, technology and services necessary to advance the protection of human health and the environment. Within the OEI, the EPA's Senior Agency Information Security Officer (SAISO) is responsible for developing, documenting, implementing and maintaining an agencywide information security program to protect EPA information and information systems. Additionally, the SAISO ensures that the agencywide information security program is in compliance with the Federal Information Security Modernization Act and related information security laws, regulations, directives, policies and guidelines.

For each program office, the Assistant Administrator and other key officials are responsible for (a) implementing the policies, procedures, control techniques and other countermeasures promulgated under the EPA Information Security Program; and (b) complying with the Federal Information Security Modernization Act and other related information security laws and requirements, in accordance with Chief Information Officer (CIO) directives. The Senior Information Official is responsible for ensuring that effective processes and necessary procedures and other directives are established to implement the policies, procedures, control techniques and other countermeasures identified under the EPA Information Security Program and enforced within their respective offices. The system owner is responsible for coordinating with the CIO, SAISO, information owners, other

[1] Cybersecurity Act of 2015, Section 406, Federal Computer Security; Pub. L. No. 2015-114-113, 129 Stat. 2574.

system owners and service managers regarding EPA Information Security Program requirements for the assigned system during its entire lifecycle. The system owner is also responsible for configuring, continuously monitoring and maintaining systems to adequately protect information stored, processed or transmitted within acceptable risks.

Scope and Methodology

We conducted this audit from March through July 2016 at EPA headquarters in Washington, D.C., 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. We believe that the information obtained provides a reasonable basis for our conclusions based on our audit objective.

We collected EPA policies and procedures related to the areas being reported under this statute. Where the EPA had not documented its processes, we relied upon information provided by the EPA and selected EPA system owners to explain the respective processes necessary to complete the report on covered systems required under this statute. To gain an understanding of the EPA service provider's implementation of its information security program, we reviewed the independent auditor's report that governs the review of the service provider's processes for protecting the data received by the EPA.

We reviewed the reporting requirements under the Cybersecurity Act of 2015, and summarized information on the EPA's existing security policies and procedures, multifactor authentication, management practices, and capabilities. We interviewed the SAISO and analyzed documentation provided by OEI. We judgmentally selected for review the following two active agency systems (Table 1) that contain sensitive PII and analyzed documentation provided by the system owners.

Table 1: Active agency systems reviewed

System name	Responsible office	System description
[redacted]	Office of Administration and Resources Management	[redacted]
[redacted]	Office of the Chief Financial Officer	[redacted]

Source: OIG analysis.

Where the act asked if appropriate standards were followed, our audit work consisted of determining whether the EPA developed its policies and procedures using current federal guidance. Specifically, we reviewed the EPA Information Security National Rules of Behavior and the EPA Information Security Policy. We analyzed the criteria within the "Authority" section of each document to

determine whether the criteria referenced within each document was based on the most current federal guidance.

We obtained and summarized relevant OIG reports on covered systems and contractor systems from fiscal years 2014 through 2016. We summarized the status of the corrective actions associated with these reports based on information contained within the agency's Management Audit Tracking System.

Prior Reports

During fiscal years 2014 through 2016, the OIG issued five audit reports on EPA practices for protecting PII and overseeing contractors that own or operate information technology systems on behalf of the agency. As noted in Table 2, we issued 19 recommendations. Based on the data in the agency's audit tracking system, the EPA has completed 79 percent (15 of 19) of these recommendations.

Table 2: Status of recommendations (based on data in the EPA's Management Audit Tracking System as of July 25, 2016)

OIG report	No. of recommendations	Completed	Not completed
1. Report No. 14-P-0122	7	7	0
2. Report No. 14-P-0323	0	-	-
3. Report No. 15-P-0290	5	2	3*
4. Report No. 15-P-0295	7	6	1**
5. Report No. 16-P-0039	0	-	-
Total: 5 reports	**19**	**15**	**4**

Source: OIG analysis.

*As of July 25, 2016, three uncompleted recommendations were current as they had not reached their planned milestone dates.
** As of July 25, 2016, this one uncompleted recommendation passed its planned milestone date and was overdue.

Below is a summary for each report.

1. **EPA Needs to Improve Safeguards for Personally Identifiable Information (Report No. 14-P-0122, dated February 24, 2014)**: This audit found that the EPA has not created formal policies and procedures for several processes that contribute to the safeguarding of PII and that ensure compliance with federal requirements. The audit also found that the EPA uses an inaccurate list of systems that contain sensitive PII to report to the U.S. Office of Management and Budget and the EPA's CIO.

2. **EPA Is Not Fully Aware of the Extent of Its Use of Cloud Computing Technologies (Report No. 14-P-0323, dated July 24, 2014**): This audit found that the EPA needs to improve the oversight process for prime contractors (to include ensuring subcontractors comply with federal security requirements and establishing service-level agreements for cloud services). The report also found that there is no assurance that the EPA has access to the subcontractor's cloud environment for audit and investigative purposes. Further, the audit found that the subcontractor is not compliant with the Federal Risk and Authorization Management Program.

3. **Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance (Report No. 15-P-0290, dated September 21, 2015**): This audit found that personnel with oversight responsibilities for contractor systems were not aware of the requirements outlined in EPA information security procedures, which resulted in EPA contractors not conducting the required annual security assessments, not providing security assessment results to the agency for review, and not establishing the required incident response capability.

4. **EPA Needs to Improve the Recognition and Administration of Cloud Services for the Office of Water's Permit Management Oversight System (Report No. 15-P-0295, dated September 24, 2015**): This audit found that inadequate oversight of the contractor resulted in inadequate controls over EPA data. In particular, the EPA failed to establish adequate requirements for hosting the application, resulting in it being hosted in a cloud service provider's environment that did not comply with federal security requirements. There was also no assurance that the EPA has access to the service provider's cloud environment for audit and investigative purposes. In addition, the service provider's terms of service were not compliant with the Federal Risk and Authorization Management Program.

5. **Fiscal Year 2015 Federal Information Security Modernization Act Report – Status of EPA's Information Security Program (Report No. 16-P-0039, dated November 16, 2015**): This audit found that although the EPA has guidance in place for oversight of contractor systems, significant improvements are needed to: (1) ensure contractors comply with required security controls; (2) maintain an accurate inventory of contractor systems; and (3) identify contractor systems that interface with the EPA systems.

Results of Review

In response to the information requested under Section 406 of the Cybersecurity Act, we determined that the agency:

- Has logical access policies and procedures for covered systems.
- Requires the use of logical access controls and multifactor authentication for privileged users to access covered systems.
- Has implemented, or is in the process of implementing, the information security management practices referred to in the act.

"**Multi-factor authentication** – The use of not fewer than two authentication factors, such as:

(a) Something that is known to the user, such as a password or personal identification number.
(b) An access device that is provided to the user, such as a cryptographic identification device or token.
(c) A unique biometric characteristic of the user."

"**Privileged User** – A user who has access to system control, monitoring or administrative functions."

Cybersecurity Act of 2015, Section 406(a)(4-5)

We limited our review to the reporting requirements under the Cybersecurity Act of 2015 and did not conclude on the quality of the policies and procedures protecting systems with PII in the agency. We are providing the following information based on the requirements outlined in Section 406(b)(2) of the act.

(A) A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

Logical access control is a process of granting or denying specific requests to obtain and use information and related information-processing services. The EPA has six policies and procedures related to logical access controls, as shown in Table 3 (along with their descriptions).

Table 3: EPA policies and procedures related to logical access, and descriptions

EPA policies and procedures	Description
CIO 2150.3, EPA Information Security Policy, August 6, 2012	"This policy establishes a program to provide security for EPA information and information systems. This is the formal, foundational policy from which all procedures, standards, guidelines and other EPA directives will be developed in defining and implementing information security requirements for EPA."
CIO 2150-P-22.0, Information Security – Privacy Procedures, July 13, 2015	"This procedure implements the Privacy information system security controls requirements identified in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST 800-53)."
CIO 2151.1, Privacy Policy, September 14, 2015	"This policy establishes the EPA requirements for safeguarding PII and Privacy Act information in accordance with the Privacy Act of 1974, the E-Government Act of 2002, and policy and guidance issued by the President and Office of Management and Budget."

EPA policies and procedures	Description
CIO 2150-P-21.0, Information Security – National Rules of Behavior, September 14, 2015	"This procedure establishes the EPA National Rules of Behavior to comply with Office of Management and Budget Circular A-130, Appendix III, paragraph 3(a(2)(a), regarding rules of behavior for users of information systems. This document is applicable to all users of EPA information and information systems. This document states it is designed to safeguard EPA information and information systems from misuse, abuse, loss or unauthorized access."
CIO 2150-P-01.2, Information Security – Access Control Procedure, September 21, 2015	"This procedure implements the Access Control information system security controls requirements identified in NIST 800-53."
CIO 2120-P-07.2, Information Security – Identification and Authentication Procedure, November 30, 2015	"This procedure implements the Identification and Authentication information system security controls requirements identified in NIST 800-53."

Source: OIG analysis.

We determined that the criteria referenced in the "Authority" sections of the EPA Information Security – National Rules of Behavior, and the EPA's Information Security Policy, are based on current federal guidelines. Therefore, we believe that appropriate standards were followed.

(B) A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

The EPA's CIO issued the EPA's Information Security – Identification and Authentication Procedure, and the Information Security – Access Control Procedure. These procedures outline the security control requirements for the identification, authentication and access control information system security controls identified in NIST Special Publication 800-53. These procedures state that all agency information systems must meet the security requirements as specified within these documents.

On July 30, 2015, the EPA's SAISO issued a memorandum, [redacted]. This memorandum requires all privileged users, by August 31, 2015, to use Personal Identification Verification [redacted]

[redacted]

- The EPA system requires the use of a Personal Identification Verification card and a Personal Identification Number (PIN) for logical access to the network.

- [redacted]

Furthermore, the security plan for one of the sampled systems indicated that:

[redacted]

For our two sampled systems, EPA management outlined within their respective system security plan that the office implemented one or more of following logical access controls identified in NIST Special Publication 800-53:

[redacted]

(C) If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

The agency requires the use of logical access controls and multifactor authentication for privileged users to access a covered system. [redacted]

(D)(i) [A description of] the policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

The agency has three policies and procedures related to conducting inventories of the software present on the covered systems and the licenses associated with such software. Those three policies and procedures, along with descriptions, are in Table 4.

Table 4: EPA policies and procedures related to conducting inventories of software present on covered systems, and descriptions

EPA policies and procedures	Description
CIO-2104.1, Software Management and Piracy Policy, January 26, 2010	"This policy establishes and describes the EPA approach to complying with Executive Order 13103 (September 30, 1998) on Computer Software Piracy. The primary purpose of this policy is to ensure that all EPA-approved software is appropriately licensed, is approved for use, and is not pirated software."
CIO-2104.0-P-01.0, Software Management and Piracy Procedure, January 26, 2010	"This procedure describes the process EPA program offices and regions must follow to comply with the EPA Software Management and Piracy Policy; and Executive Order 13103, Computer Software Piracy. This procedure is based on the Federal CIO Council's guidelines."
CIO 2104-G-01.0, Guidelines for the Software Management and Piracy Policy, June 13, 2003	"EPA's Software Management and Piracy Policy requires the EPA to acquire, manage and use computer software in compliance with applicable laws and licensing restrictions to guard against use of counterfeit software or software that violates licensing restrictions. Mismanagement of copyrighted and/or licensed computer software conflicts with fundamental government and EPA values regarding protection of intellectual property. These guidelines, based on the Federal CIO Council's guidelines, give recommendations for implementing the Policy and Executive Order 13103 on Computer Software Piracy."

Source: OIG analysis.

The EPA policies and procedures state that:

- Each program office or region must establish and maintain an auditable procedure to ensure that all software purchased or acquired, and all software installed on EPA computer systems, adheres to the EPA's Software Management and Piracy Policy.
- Only software that is properly licensed and approved for use may be installed on EPA computer systems, including personal computers and servers.
- The EPA Software Management and Piracy Policy, and the EPA Software Management and Piracy Procedure, are applicable to all users of EPA-owned or leased computers, systems, and/or software. EPA contractors and recipients of EPA federal financial assistance must adhere to this policy and procedure.

(D)(ii) [A description of the] capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including: Data loss prevention capabilities; Forensics and visibility capabilities; or Digital rights management capabilities.

The agency also has the following procedures that address forensics and visibility capabilities:

- CIO 2150-P-08.2, Information Security - Incident Response Procedures.
- CIO 2150.3-P-17.1, Information Security- Interim System and Information Integrity Procedures.

Additionally, as of June 2016, the agency was developing a draft Data Loss Prevention procedure. [redacted]

EPA representatives indicated they use the following capabilities to monitor and detect exfiltration and other threats (Table 5).

Table 5: EPA capabilities to monitor and detect exfiltration and other threats

Data loss prevention capabilities	Forensics and visibility capabilities	Digital rights management capabilities
[redacted]	[redacted]	[redacted]

Source: OIG analysis.

In addition to the capabilities OEI describes in its responses to Section (D)(ii) above, the EPA representative from one of the two sampled systems indicated the office uses the following capabilities associated with the sampled system to monitor and detect exfiltration and other threats (Table 6).

Table 6: Additional capabilities to monitor and detect exfiltration and other threats to a sampled system

Data loss prevention capabilities	Forensics and visibility capabilities	Digital rights management capabilities
• [redacted]	[redacted]	[redacted]

Source: OIG analysis.

(D)(iii) A description of how the covered agency is using the capabilities described in clause (ii).

The following describe how EPA representatives indicated the agency is using the capabilities to monitor and detect exfiltration and other threats.

Data Loss Prevention Capabilities

[redacted]

Forensics and Visibility Capabilities

[redacted]

[redacted]

Digital Rights Management Capabilities

[redacted]

(D)(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

[redacted]

(E) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency, are implementing the information security management practices described in subparagraph (D).

The EPA's Software Management and Piracy policy and procedure provide the policy, procedures, standards and guidance to senior-level managers to support agency requirements and manage enterprise software licenses. These agency documents state that all users of EPA-owned or leased computers, systems and/or software must adhere to this guidance, as well as EPA contractors and recipients of EPA federal financial assistance.

Additionally, the EPA's Information Security Policy specifies that it is the formal, foundational policy from which all procedures, standards, guidelines and other directives will be developed in defining and implementing information security requirements for the agency. This policy covers all EPA information and information systems, to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the agency. The policy states it applies to all EPA employees and contractors, and all other users of EPA information and information systems.

Based on previously completed work for our annual audit of the EPA's consolidated financial statements, we obtained and reviewed the independent auditor's report provided by KPMG, LLC. The *Report on the U.S. Department of Interior's Description of Its Federal Personnel and Payroll System and the Suitability of the Design and Operating Effectiveness of Its Controls* (SSAE 16 – Type 2 Report) was issued for the period July 1, 2014, to June 30, 2015. The report covers a review of the controls for one of the EPA's service providers that operate a major financial application on behalf of the agency. The KPMG, LLC independent auditor's opinion stated:

> In our opinion, in all material respects, based on the criteria described in Interior's assertions, (1) the description fairly presents the system was designed and implemented throughout the period July 1, 2014 through June 30, 2015, (2) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved…, and (3) the controls tested … if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2014 through June 30, 2015.

EPA Response to the Draft Report and OIG Evaluation

Due to the critical milestones necessary to meet the act's mandatory reporting date, we worked closely with EPA representatives throughout this audit to obtain the data contained within this report, and to ensure the EPA was familiar with the findings and issues addressed in the draft report. On July 20, 2016, we met with EPA representatives to discuss the factual accuracy of our draft report.

The EPA's Office of Administration and Resources Management verbally concurred with the information in our draft report, and indicated that the EPA will not provide a written response.
The EPA's Office of Chief Financial Officer also agreed with the report, and provided us documentation to support that the office created a plan of action and milestones to track the remediation of the reviewed application's weakness related to multifactor authentication.

The EPA's OEI mostly agreed with the audit results, and emailed us comments related to the following areas:

- For Table 2, OEI said the OIG should indicate how many of the unimplemented recommendations were late and update the status of the recommendations, as the office took additional actions on the recommendations subsequent to the date the table was created.

- OEI outlined what measures the agency has in place for addressing data loss prevention and digital rights management. OEI also made us aware of two additional agency procedures that address the agency's forensics and visibility capabilities.

In response to these comments, we updated Table 2 with the status of the open recommendations as of July 25, 2016. We also updated our discussion regarding Section (D)(ii), and made other minor editorial changes to the report to address OEI comments. We provided the updated report language to OEI, and OEI indicated the language was correct.

Appendix A

Distribution

Office of the Administrator
Chief Information Officer, Office of Environmental Information
Assistant Administrator, Office of Administration and Resources Management
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Principal Deputy Assistant Administrator, Office of Environmental Information
Principal Deputy Assistant Administrator, Office of Administration and Resources Management
Senior Agency Information Security Officer, Office of Environmental Information
Audit Follow-Up Coordinator, Office of Environmental Information
Audit Follow-Up Coordinator, Office of Administration and Resources Management
Audit Follow-Up Coordinator, Office of the Chief Financial Officer