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

OFFICE OF
INSPECTOR GENERAL

March 14, 2016

MEMORANDUM

SUBJECT: Project Notification:
Audit of EPA's Protection of Systems With Access to National Security or Personally Identifiable Information
Project No. OA-FY16-0126

FROM: Rudolph M. Brevard, Director
Information Resources Management Audits
Office of Audit

Rudolph M. Brevard

TO: *See Below*

The U. S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), plans to begin fieldwork for an audit of the EPA's compliance with the mandated "Inspector General Report on Covered Systems," as outlined in the Cybersecurity Act of 2015.

The OIG's audit objective is 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, as outlined in Title IV, Section 406 of the Cybersecurity Act of 2015. The OIG plans to conduct its work at EPA headquarters and at other EPA offices as needed. Applicable generally accepted government auditing standards will be used in conducting our project. The anticipated benefit of this project is to contribute to the agency's theme of "Embracing EPA as a High-Performing Organization."

We will contact you to arrange a mutually agreeable time to discuss the audit scope and objective. We would also be particularly interested in any areas of concern that you may have. We will answer any questions you may have about the project process, reporting procedures, methods used to gather and analyze data, and what we should expect of each other during the course of the project. During the audit, we will provide updates on a regular basis by email, and/or during meetings with the Senior Agency Information Security Officer and appropriate program and regional audit follow-up coordinators.

Attachment A contains a listing of specific information that we need from the EPA in order to complete the Inspector General Report on Covered Systems, and additional information needed from select EPA system owners. To ensure the success and timely completion of this project, the EPA should provide the OIG with the requested information in Attachment A within 2 weeks from the date of this memo.

We respectfully note that the OIG is authorized by the Inspector General Act of 1978 to have timely access to personnel and all materials necessary to complete its objectives. We will request your resolution if an agency employee or contractor refuses to provide requested records to the OIG, or otherwise fails to cooperate with the OIG. We may report unresolved access matters to the Administrator and include the incident in the Semiannual Report to Congress.

I will be supervising the project, and any information related to the project should be addressed to me at (202) 566-0893 or brevard.rudy@epa.gov; or to Chuck Dade, Project Manager, at (202) 566-2575 or dade.chuck@epa.gov.

Attachments (2)

Addressees
Donna Vizian, Acting Assistant Administrator, Office of Administration and Resources Management
David Kling, Acting Associate Administrator for Homeland Security, Office of the Administrator
Ann Dunkin, Chief Information Officer, Office of Environmental Information
Jackie Brown, OASIS System Owner, Office of Administration and Resources Management
Quentin Jones, SCORPIOS System Owner, Office of the Chief Financial Offer

cc: Gina McCarthy, Administrator
Mike Kenyon, Acting Principal Deputy Assistant Administrator, Office of Environmental Information
David Bloom, Acting Chief Financial Officer, Office of the Chief Financial Officer
Robert McKinney Jr., Senior Agency Information Security Officer, Office of Environmental Information
Harrell Watkins, Acting Director, Office of Technology Operations and Planning, Office of Environmental Information
Nic Grzegozewski, Agency Follow-Up Coordinator
Brandon McDowell, Audit Follow-Up Coordinator, Office of Administration and Resources Management
Glen Cuscino, Audit Follow-Up Coordinator, Office of the Administrator
Judi Maguire, Audit Follow-Up Coordinator, Office of Environmental Information
Lorna Washington, Audit Follow-Up Coordinator, Office of the Chief Financial Officer
Melissa Harrison, Press Secretary, Office of Public Affairs
Arthur A. Elkins Jr., Inspector General
Charles Sheehan, Deputy Inspector General
Aracely Nunez-Mattocks, Chief of Staff, Office of Inspector General
Alan Larsen, Counsel to the Inspector General
Kevin Christensen, Assistant Inspector General for Audit
Carolyn Copper, Assistant Inspector General for Program Evaluation
Patrick Sullivan, Assistant Inspector General for Investigations
Rich Eyermann, Deputy Assistant Inspector General for Audit
Jennifer Kaplan, Deputy Assistant Inspector General for Congressional and Public Affairs
Jeffrey Lagda, Congressional and Media Liaison, Office of Inspector General

Attachment A

Request for Information

Office of Homeland Security (OHS)

For OHS, please provide a list of any EPA National Security systems.

If any EPA National Security systems exist, please provide the following (in electronic format):

(A)

1) A description of the logical access policies and practices of the National Security systems.
2) Copies of the policies and procedures that address logical access to the National Security systems.

(B) A description and list of the logical access controls and multi-factor authentication used by the EPA for privileged users of the National Security systems.

(C)

1) If the Agency is not using logical access controls to access National Security system, please provide a description of the reasons for not using logical access controls.
2) If the Agency is not using multi-factor authentication to access National Security system, please provide a description of the reasons for not using multi-factor authentication.

(D)

1) A description of the policies and procedures followed to conduct inventories of software present on covered systems and licenses associated with such software.
2) Copies of the policies and procedures associated with the practices followed for conducting inventories of the software present and the licenses associated with such software.
3) A description of the capabilities the Agency utilizes to monitor and detect exfiltration and other threats, including: (a) data loss prevention capabilities, (b) forensics and visibility capabilities, and (c) digital rights management capabilities, with respect to National Security systems.
4) A description of how the Agency is using the capabilities described in item (D) 3 above.
5) If the Agency is not utilizing capabilities described in item (D) 3 above, please provide a description of the reasons for not utilizing such capabilities.

(E)

1) A description of the policies and practices the Agency uses with respect to ensuring that entities, including contractors, that provide services to the EPA are implementing the information security management practices described in (D) above.
2) Copies of the policies and procedures associated with these policies and practices.

Office of Environmental Information (OEI)

For OEI, please provide the following (in electronic format):

(A)

1) A description of the logical access policies and practices of covered systems.
2) Copies of the policies and procedures that address logical access to Agency covered systems.

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

(C)

1) If the Agency is not using logical access controls to access covered systems, please provide a description of the reasons for not using logical access controls.
2) If the Agency is not using multi-factor authentication to access covered systems, please provide a description of the reasons for not using multi-factor authentication.

(D)

1) A description of the policies and procedures followed to conduct inventories of software present on covered systems and licenses associated with such software.
2) Copies of the policies and procedures associated with the practices followed for conducting inventories of the software present and the licenses associated with such software.
3) A description of the capabilities the Agency utilizes to monitor and detect exfiltration and other threats, including: (a) data loss prevention capabilities, (b) forensics and visibility capabilities, and (c) digital rights management capabilities, with respect to the covered systems.
4) A description of how the Agency is using the capabilities described in item (D) 3 above.
5) If the Agency is not utilizing capabilities described in item (D) 3 above, please provide a description of the reasons for not utilizing such capabilities.

Office of Administration and Resources Management (OARM)

For OARM, please provide the following (in electronic format):

(E) A description of the policies and practices EPA uses with respect to ensuring that entities, including contractors, that provide services to EPA are implementing the following information security management practices:

1) Information security management practices used to conduct inventories of the software present on the systems and the licenses associated with such software.
2) Information security management practices used to monitor and detect exfiltration and other threats, including: (a) data loss prevention capabilities, (b) forensics and visibility capabilities, and (c) digital rights management capabilities.
3) Copies of the EPA's policies and procedures associated with these policies and practices.

System Owners of OASIS (OARM) and SCORPIOS (OCFO) Request for Information

We selected two systems to review: (1) OARM's Office of Administration Services Information System (OASIS); and (2) OCFO's Superfund Cost Recovery Package Imaging Online System (SCORPIOS).

For the system owners of OASIS and **SCORPIOS, please provide (in electronic format)**:

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

(C)

1) If the Agency is not using logical access controls to access the applicable system, please provide a description of the reasons for not using logical access controls.
2) If the Agency is not using multi-factor authentication to access the applicable system, please provide a description of the reasons for not using multi-factor authentication.

(D)

1) A description of the policies and procedures followed to conduct inventories of software present on applicable system and licenses associated with such software.
2) Copies of the policies and procedures associated with the practices followed for conducting inventories of the software present and the licenses associated with such software.
3) A description of the capabilities the Agency utilizes to monitor and detect exfiltration and other threats for the applicable system, including: (a) data loss prevention capabilities, (b) forensics and visibility capabilities, and (c) digital rights management capabilities, with respect to the covered systems.
4) A description of how the Agency is using the capabilities described in item (D) 3 above.
5) If the Agency is not utilizing capabilities described in item (D) 3 above, please provide a description of the reasons for not utilizing such capabilities.

Attachment B

Excerpt From the Cybersecurity Act of 2015

SEC. 406. FEDERAL COMPUTER SECURITY.

(a) DEFINITIONS.—In this section:

(1) COVERED SYSTEM.—The term ‘‘covered system’’ shall mean a national security system as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.

(2) COVERED AGENCY.—The term ‘‘covered agency’’ means an agency that operates a covered system.

(3) LOGICAL ACCESS CONTROL.—The term ‘‘logical access control’’ means a process of granting or denying specific requests to obtain and use information and related information processing services.

(4) MULTI-FACTOR AUTHENTICATION.—The term ‘‘multifactor authentication’’ means the use of not fewer than 2 authentication factors, such as the following:

(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.

(5) PRIVILEGED USER.—The term ‘‘privileged user’’ means a user who has access to system control, monitoring, or administrative functions.

(b) INSPECTOR GENERAL REPORTS ON COVERED SYSTEMS.—

(1) IN GENERAL.—Not later than 240 days after the date of enactment of this Act, the Inspector General of each covered agency shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report, which shall include information collected from the covered agency for the contents described in paragraph (2) regarding the Federal computer systems of the covered agency.

(2) CONTENTS.—The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:

(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.

(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.

(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.

(D) A description of the following information security management practices used by the covered agency regarding covered systems:

(i) 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.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—
(I) data loss prevention capabilities;
(II) forensics and visibility capabilities; or
(III) digital rights management capabilities.

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

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

(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).