U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Information Technology

Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance

Report No. 15-P-0290 **September 21, 2015**

Scan this mobile code to learn more about the EPA OIG.

Report Contributors:

Rudolph M. Brevard
Vincent Campbell
Scott Sammons
Teresa Richardson

Abbreviations

CIO	Chief Information Officer
COTS	Commercial-Off-the-Shelf
EEO	Equal Employment Opportunity
EPA	U.S. Environmental Protection Agency
GOTS	Government-Off-the-Shelf
GSS	General Support Systems
HRLOB	Human Resource Line of Business
IT	Information Technology
OIG	Office of Inspector General
PRIS	Peer Reviewer Information System
READ	Registry for EPA Applications and Databases
SLCM	System Life Cycle Management

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

U.S. Environmental Protection Agency
Office of Inspector General

15-P-0290
September 21, 2015

At a Glance

Why We Did This Audit

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to determine to what extent the EPA relies on contractor systems for information processing and programmatic support, and whether the EPA has implemented management-control processes to mitigate information security risks posed by the systems.

The EPA *System Life Cycle Management (SLCM) Procedure* details the system development phases, activities and documents necessary to properly manage and control the agency's information technology (IT) investments.

The EPA uses IT systems operated and maintained by contractors to conduct information collection and analysis. We learned from EPA OIG investigators that data maintained by a third party and residing at the vendor's site were breached on multiple occasions.

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.

The full report is at:
www.epa.gov/oig/reports/2015/20150921-15-P-0290.pdf

Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance

What We Found

Agency officials were unaware of which systems or services are required by the SLCM Procedure to be included in the EPA's authoritative information system database known as the Registry of EPA Applications, Models and Databases (READ). The READ inventory is important because it provides the tracking mechanism to ensure IT investments receive the appropriate level of oversight.

By not having a complete inventory of contractor systems, and by not assessing the operating effectiveness of contractor control environments in which systems are placed, the EPA risks being unable to protect its resources and data from undue harm.

Officials were also unaware of which stage of the system life cycle to enter contractor systems into READ, and in cases where multiple offices manage separate components of the same contractor system, which program office is responsible for updating READ. As a result, READ did not contain information on 22 contractor systems that are owned or operated on behalf of the EPA and are located outside of the agency's network. The registry also lacked information on 81 internal EPA contractor-supported systems.

We also found that personnel with oversight responsibilities for contractor systems were not aware of the requirements outlined in EPA information security procedures. As a result, EPA contractors did not conduct the required annual security assessments, did not provide security assessment results to the agency for review, and did not establish the required incident response capability. Without the required security controls, data breaches costing from $1.4 million to over $12 million could have occurred if all files within these systems were compromised.

Recommendations and Planned Agency Corrective Actions

We recommend that the Chief Information Officer update the 2015 READ data call instructions to include language from the agency's SLCM procedure. We also recommend that the Assistant Administrator for Administration and Resources Management designate responsible individual(s) to be the Primary Information Resource Steward(s) for READ records for the systems that comprise the Human Resources Line of Business, throughout the systems' life cycle.

In addition, we recommend that the Chief Information Officer implement the previously approved EPA Information Security Task Force recommendations for implementing a role-based training program, and for managing the annual security assessments and vulnerability management program. The EPA agreed with our recommendations and provided a corrective action plan with dates for each recommendation.

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

THE INSPECTOR GENERAL

September 21, 2015

MEMORANDUM

SUBJECT: Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance
Report No. 15-P-0290

FROM: Arthur A. Elkins Jr.

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

Karl Brooks, Acting Assistant Administrator
Office of Administration and Resources Management

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position.

The EPA's Office of Environmental Information and the Office of Administration and Resources Management have primary responsibility for implementing the recommendations in this report.

Action Required

In accordance with EPA Manual 2750, the agency offices provided acceptable and complete planned corrective actions in response to OIG recommendations. All recommendations are resolved and no response to this report is required.

We will post this report to our website at http://www.epa.gov/oig.

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), sought to determine to what extent the EPA relies on contractor systems for information processing and programmatic support, and whether the EPA has implemented management-control processes to mitigate information security risks posed by these systems.

Background

The EPA uses information technology (IT) systems operated and maintained by third parties to conduct information collection and analysis. We learned from EPA OIG investigators that data maintained by a third party and residing at the vendor's site were breached on multiple occasions. Managerial oversight of contractor compliance with information security control is critical for maintaining the public's confidence in the environmental impacts achieved through EPA programs, as well as for helping to avoid costs associated with data breaches.

The EPA's Information Security Policy specifies that agency Assistant Administrators and Regional Administrators are responsible for ensuring that all employees within their organizations take immediate action to comply with directives from the Chief Information Officer (CIO), including requirements to:

- Mitigate the impact of any potential information security risk.
- Respond to an information security incident.
- Implement provisions of the EPA's Network Security Operations Center notifications.

According to benchmark research sponsored by an award-winning technology company, and conducted by the Ponemon Institute in May 2013, the average cost of a data breach for a public sector system without financial information is $142 per record. The study found that key factors, such as having a formal incident response plan and security assessment testing of a system's security posture, decreases the cost per compromised record. For example, the Ponemon Institute concluded that having an incident response plan can lower the cost of a compromised record to $100.

Responsible Offices

The following EPA offices are responsible for taking action on the recommendations in this report:

- Office of Environmental Information.
- Office of Administration and Resources Management.

Scope and Methodology

We performed this audit from April 2014 through June 2015. We performed this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

For the purposes of this audit, "contractor systems" are IT systems and application projects that are owned or operated on behalf of the EPA by contractors, and located outside of the agency's network. This includes both applications and general support systems (GSS); custom developed, commercial-off-the-shelf (COTS) or government-off-the-shelf (GOTS) projects; and cloud-based solutions.

We reviewed EPA policies and procedures related to maintaining contractor system inventory. We surveyed all EPA program and regional offices in order to compile a listing of EPA contractor systems. We interviewed agency officials and representatives to review their survey responses and to determine the accuracy of their responses. We analyzed and compared the results of the survey to the EPA's authoritative information system database, known as the Registry of EPA Applications, Models and Databases (READ), to determine if the agency was accurately tracking contractor systems managed or hosted on its behalf. We also reviewed agency and federal guidelines for protecting and implementing information system security controls for systems managed or hosted on behalf of the agency.

Using the analysis produced from our survey, we judgmentally selected and tested security controls for contractor systems that met at least one of the following criteria: 1) known security breaches; and 2) systems contained in the EPA's listing of Systems of Records Notice.[1] The systems we selected for testing are listed in Table 1.

[1] Agencies are required to publish a System of Records Notice in the Federal Register upon the establishment of, or the substantial revision of, a group of records containing information covered under the Privacy Act.

Table 1: EPA contractor systems selected for testing

System name	Program office	System description
Peer Reviewer Information System (PRIS)	Office of Research and Development	Database of potential peer reviewers and information about their areas of specialization, highest degrees, work address, and electronic contact information for people who have authorized the EPA to retain this data in compliance with the Privacy Act.
iStar	Office of Air and Radiation	Database that contains information about partners and Energy Star labeled products. Information from this database is posted on the Energy Star website and refreshed frequently.
iComplaints	Office of the Administrator	An equal employment opportunity (EEO) complaint tracking system that manages the EEO process and generates annual reports, manages EEO complaints and cases, and ensures the agency is in compliance with all regulatory reporting requirements and mandates.

Source: Information compiled by the OIG.

We interviewed agency and contractor points of contact responsible for and knowledgeable about the security posture of these contractor systems, and requested documentation related to incident response handling and security assessments. We performed the following steps on the documentation that was received:

- **We reviewed incident response plans** to determine if the plans met criteria documented in the EPA's Interim Incident Response Procedures. Appendix C lists the specific incident response elements tested. We reviewed incident response tracking documentation to ensure incidents were monitored and tracked.

- **We reviewed contractors' security assessment plans and assessment reports** to determine if the plans met criteria documented in the EPA's *Interim Security and Authorization Procedures*. Appendix C lists the specific security assessment requirements tested. We reviewed contractual documentation to determine what type of security assessment is expected, and if specific language required the contractor to provide security assessment results to the EPA. We interviewed authorizing officials to determine if they requested results from the security assessment report; and if so, did the report's results inform them of any security weaknesses associated with the system.

In addition, we calculated the estimated cost of a data breach for the systems we tested by using information produced by benchmark research sponsored by an award-winning technology company, and conducted by the Ponemon Institute in May 2013. We used the reported cost associated with a data breach to a public-

sector system and factored out costs associated with identity protection services, since the systems tested did not contain personal financial information. We also adjusted the costs for risk mitigating factors associated with each tested system. We relied on records counts for each system provided by the agency. We did not conduct any additional testing of system controls to verify the integrity of the systems' processing environment. However, we did verify whether the system had a current system security assessment and whether management was aware of any weaknesses associated with the system.

Prior Audit Work

We followed up on EPA OIG Report No. 2007-P-00007, *EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents*, issued January, 11, 2007. In the 2007 report, we recommended that the agency address weaknesses associated with contractor systems, and assign duties and responsibilities for maintaining and updating information posted on the EPA's website. We also recommended that the EPA update its guidance for identifying contractor systems. Our audit disclosed that the EPA made sufficient progress updating information posted on its website, and improving agency guidance for identifying contractor systems.

Our 2007 report also recommended that the EPA establish formal procedures to ensure that all responsible program offices update and maintain their EPA-specific contract clauses on a regular basis. Based on Management Audit Tracking System data, the agency indicated the recommendations were completed April 9, 2007.

However, in this current audit we found that the EPA's contract language is still vague. Our audit identified the need for specificity in the areas of incident response capability and security assessment requirements.

Chapter 2
EPA Lacks a Complete Inventory of Contractor Systems

The EPA's inventory of contractor systems is incomplete. According to the EPA's CIO 2121-P-03.0, *System Life Cycle Management (SLCM) Procedure*, dated September 21, 2012, all IT systems, including contractor systems, should be entered and updated in the agency's official system inventory registry known as READ. However, our audit disclosed a lack of awareness regarding policy and procedure requirements. Further, we found that the SLCM procedure document lacked instructions for handling situations where programs share a contractor system. Without a complete inventory, the agency cannot ensure that contractor systems receive the required IT governance to mitigate risks to the efficacy of contractor system data, or ensure the systems address agency legal requests.

Better Inventory Reporting Practices Are Needed

The EPA's official IT systems inventory does not contain all contractor systems as required by the EPA's SLCM procedure dated September 21, 2012. We surveyed each program and regional office to compile a listing of contractor systems. Our analysis of this list showed that 22 contractor systems and an initiative were not reported in READ. Table 2 lists the systems and the initiative.

Prior to reporting, the agency provided evidence on March 4, 2015, that all components of the Human Resource Line of Business Initiative (headed by the Office of Personnel Management) had been entered into READ. We list additional information on this initiative in Table 2, number 22.

Although our audit focus was contractor systems external to the agency's network, our analysis identified 81 internal EPA contractor-supported systems that were not reported in READ. The internal contractor-supported systems are listed in Appendix D.

Table 2: Contractor systems not reported in READ

EPA Office	Number	System Name/Initiative
Office of the Chief Financial Officer	1	Concur
Office of Environmental Information	2	ECSS-FAQS
	3	Adobe Connect
Office of General Counsel	4	LexisNexis Legal Research Service
Office of Research and Development	5	Google Apps
	6	Research Line Source Model for Near Surface Release
	7	Environmental Technology Verification Program
	8	Municipal Solid Waste Decision Support Tool
	9	Nitrogen–A simple geospatial model of watershed nitrogen
Office of Research and Development	10	Envision
	11	STAA
	12	AgDrift
	13	Data for Environmental Modeling
	14	Human and Ecological Exposure and Risk in Multimedia Environmental Systems
	15	Message Development for Water Contamination
	16	Provisional Advisory Level
	17	Ubertool: Ecological Risk Application for Pesticide Modeling
Office of Water	18	OW Enterprise Project Management
	19	NHD Plus Dataset-Federal Geographic Data Committee
	20	Urban Waters Mapper
Region 6	21	EPA Response Manager
Shared Contractor System: **Office of the Chief Financial Officer** **Office of Environmental Information** **Office of Administration and Resources Management**	22	Components of the Human Resource Line of Business Initiative (HRLOB); Headed by Office of Personnel Management. Examples of HRLOB components are DataMart, WTTS, and EODS. Note: The preceding components are a partial list of HRLOB components. The remaining components were recorded in READ.

Source: Information compiled by the OIG.

The EPA's *System Life Cycle Management Procedure* documents steps for entering and updating a record in the agency's system inventory registry (READ) for every phase of the SLCM (i.e., definition through termination). The EPA's CIO 2121.1, *System Life Cycle Management Policy*, also dated September 21, 2012, specifies that system owners and managers are responsible for monitoring compliance with SLCM guidance, and for providing day-to-day management of the system life cycle process and products within their programs.

Responsible Individuals Are Unaware of the SLCM Procedure

Many agency officials are not aware of which systems or services are required by the SLCM procedure to be included in the inventory. When asked, agency officials were unaware that the SLCM procedure applies to:

> …all EPA IT systems and application projects, both applications and general support systems (GSS). It is applicable to custom developed, commercial-off-the-shelf (COTS), or government-off-the-shelf (GOTS) projects and applies to applications developed for mobile devices. It also applies to systems developed on behalf of EPA by contractors irrespective of where the IT systems are hosted; including cloud-based solutions.

In addition, agency representatives were not aware of when to enter contractor systems into READ, even though the SLCM procedure requires the system inventory to be updated during every phase of the system life cycle (i.e., definition through termination). Further, it was unclear whether contractor services that help support an office's business need and mission should be included in READ (e.g., LexisNexis Legal Research Services and Google Apps). Agency officials were also unclear as to which program office was responsible for updating READ in cases where multiple offices manage separate components of the same contractor system.

For example, the EPA created a memorandum of understanding outlining security responsibilities for its Human Resources Line of Business Initiative. However, the EPA did not create a similar memorandum of understanding or appoint someone in writing to govern administrative tasks associated with the project. As a result, only portions of the project's components were recorded in READ.

While the EPA's SLCM procedure requires READ to be updated, agency Senior Information Officials are notified to update READ via an annual memorandum titled *Data Call for Registry of EPA Applications, Models and Databases.* Our review of the data call memorandum revealed that the instructions do not mention contractor systems, define contractor systems, or contain language consistent with the SLCM procedure.

Conclusion

Without a complete inventory of contractor systems, the agency cannot ensure that all IT systems, services and models are receiving the appropriate level of IT governance. Furthermore, without a complete inventory, there is no way to determine if there are systems already developed or acquired that will meet current or future information or information-processing needs. In addition, the agency risks the possibility of not providing complete responses to litigation and Freedom of Information Act requests.

Recommendations

We recommend that the Chief Information Officer:

1. Update the 2015 READ data call instructions to include:

    - Language that instructs programs to register systems developed externally but used internally, consistent with the SLCM Procedure.

    - Language from the SLCM procedure that outlines the steps for updating the READ database for contractor systems during all applicable phases of the system life cycle.

    - Instructions that request a recertification that offices have verified that all contractor systems that meet the criteria within the guidance are in READ and system records are up-to-date.

We recommend that the Assistant Administrator for Administration and Resources Management:

2. Designate responsible individual(s) to be the Primary Information Resource Steward(s) for the READ records for systems that comprise the Human Resources Line of Business Initiative, throughout the systems' life cycles.

Agency Response and OIG Evaluation

The agency concurred with our findings. Furthermore, the agency provided details related to its update of the 2015 READ data call instructions and provided additional details surrounding the roles and responsibilities for updating READ. As such, we updated Recommendations 1 and 2. The EPA concurred with the updated recommendations and provided completion dates and documentation that corrective actions had been completed. The recommendations are considered resolved with corrective actions completed.

The agency also provided general comments on the draft report related to the sponsors for the HRLOB initiative and the status of systems recorded in READ. Where appropriate, we updated our report. The agency's response is found in Appendix A.

Chapter 3
EPA's Contractor Systems May Pose Risks Due to Lack of Oversight

EPA representatives did not provide oversight of contractors managing or hosting information systems on behalf of the agency. In this regard, the EPA had not reviewed the contractors' annual security assessments, ensured contractors conducted their annual security assessments, or ensured a contractor established an incident response capability.

The EPA's guidance provides requirements for assessing security of information systems and procedures for responding to security incidents. However, agency representatives were not aware of their responsibility to oversee the implementation of this guidance. A lack of contractor oversight that ensures security assessment activities are conducted—and that incident response capabilities are in place—could result in a weak security posture, a compromised system, or the inability to subvert a data breach. As a result, the EPA could potentially spend from $1.4 million to over $12 million to mitigate data breaches on the systems we reviewed.

EPA Needs to Improve Controls Over Contractor Security Assessments and Incident Response Processes

The EPA did not implement management-control processes to mitigate information security risks posed by contractor systems. One Office of Air and Radiation system, known as iStar, had not met the EPA's security assessment requirements. Additionally, we found that the contractor managing the Peer Reviewer Information System (PRIS), an Office of Research and Development system, did not meet security assessment and incident response requirements. Specifically, the contractor:

- Had not developed a security assessment plan.
- Had not conducted a security assessment review.
- Had not developed an incident response plan.
- Did not have a process in place to track incidents.

We also reviewed an Office of the Administrator system, known as iComplaints, which had requisite security assessment and incident response processes in place. We noted that for all contractor systems reviewed, the agency did not obtain the security assessment results that are to be provided to the Authorizing Official as required by policy.

The EPA'S CIO 2150.3, *Environmental Protection Agency Information Security Policy*, dated August 6, 2012, provides the overarching direction for information security requirements, and covers all EPA information and information systems. The policy applies to information systems managed or operated by a contractor or other organizations on behalf of the agency.

One of the agency's procedures, CIO-2150.3-P-04.1, *Information Security - Interim Security Assessment and Authorization Procedures*, v2, dated July 16, 2012, states that systems will undergo a security assessment based on federal guidelines used to conduct security controls reviews, and the assessment "must be provided, in writing, to the Authorizing Official or Authorizing Official designated representative." Incident response is also covered under CIO-2150.3-P-08.1, *Information Security– Interim Incident Response Procedures*, v3.1, dated July 19. 2012, which states that a system incident response plan must be developed and incidents must be tracked and documented.

Responsible Personnel Are Unaware of Oversight Responsibilities

We found that the EPA did not provide oversight of contractors implementing EPA information security procedures, because responsible personnel were unaware of the requirements outlined in the agency's information security procedures. In addition, agency representatives lack processes to ensure contractors submit their annual IT security assessment results to EPA personnel for review.

Managerial oversight of contractor compliance with information security control is key to maintaining the public's confidence in the environmental impacts achieved through EPA programs, as well as for helping to avoid costs associated with data breaches. The Ponemon Institute study placed the average cost of a data breach for a public sector system without financial information at $142 per record. The study found that key factors, such as having a formal incident response plan and a strong security posture, decreases the cost per compromised record to $100 and $108, respectively.

The PRIS and iStar systems contain a collective total of 122,835 records. Based on those statistics and the results of our analysis, we surmise that if all the records in the two systems were compromised, the breach could cost the agency from $1.4 million to over $12 million. Table 3 shows our calculation of costs associated with a data breach.

Table 3: Calculation of costs associated with a data breach

System name	Testing results	Number of records	Cost per compromised record based on testing results	Cost of data breach
Peer Reviewer Information System (PRIS)	• Security assessment requirements not met. • No incident response plan or tracking of incidents.	10,038	$ 142	$ 1,426,199
iStar	• Security assessment requirements not met. • Incident response plan in place. • Incidents are tracked.	112,797	$ 100	$ 11,288,723
Totals		**122,835**		**$ 12,714,922**

Source: Information compiled by the OIG.

Recent Agency Action Prompted by OIG Work

On July 14, 2014, we made Office of Research and Development officials aware of missing documents needed to meet prescribed security assessment and incident response requirements. To address these issues identified during our audit, ORD on August 7, 2014, and August 12, 2014, approved an incident response plan and security assessment plan for the Peer Reviewer Information System.

Conclusion

By not assessing the operating effectiveness of contractor control environments in which systems and services are placed, the EPA risks being unable to effectively mitigate security vulnerabilities, and unable to protect the organization's resources and data from undue harm. Without management-control processes in place, federal information systems are subject to serious risks including environmental disruptions, human or machine errors, and advanced persistent threats.

Recommendations

We recommend that the Chief Information Officer:

3. Implement the previously approved EPA Information Security Task Force recommendation for implementing role-based training and credentialing programs, and include contractor oversight training as part of the programs.

4. Implement the recommendation of the EPA's Information Security Task Force to manage annual security assessments, and include steps to oversee assessments to be conducted under a centralized contract or interagency agreement.

5. Implement the recommendation of the EPA's Information Security Task Force to manage the vulnerability management program.

Agency Response and OIG Evaluation

The agency agreed with our findings. However, EPA believes it was appropriate to have an agencywide approach to managing the security responsibilities for contractor systems. The Chief Information Officer assumed the lead role in implementing a strategy and provided the OIG with proposed alternative recommendations with anticipated milestone dates to address our concerns. We reviewed the EPA's proposed actions and supporting documents, and believe that once implemented, the proposed actions will address our concerns. As such, we updated the report to show that our original four recommendations were replaced by the agency's three proposed recommendations. We consider these recommendations resolved with corrective actions pending.

The EPA also provided general comments related to how the OIG calculated the cost avoidance if the reviewed systems were compromised. Where appropriate, we updated the report. Appendix A contains the agency's response. Appendix B documents the OIG's revised recommendations and the EPA's agreed-to corrective action plan.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed-To Amount
1	8	Update the 2015 READ data call instructions to include: • Language that instructs programs to register systems developed externally but used internally, consistent with the SLCM Procedure. • Language from the SLCM procedure that outlines the steps for updating the READ database for contractor systems during all applicable phases of the system life cycle. • Instructions that request a recertification that offices have verified that all contractor systems that meet the criteria within the guidance are in READ and system records are up-to-date.	C	Chief Information Officer	5/27/15		
2	8	Designate responsible individual(s) to be the Primary Information Resource Steward(s) for the READ records for systems that comprise the Human Resources Line of Business Initiative, throughout the systems' life cycles.	C	Assistant Administrator for Administration and Resources Management	2/27/15		
3	12	Implement the previously approved EPA Information Security Task Force recommendation for implementing role-based training and credentialing programs, and include contractor oversight training as part of the programs.	O	Chief Information Officer	9/30/16		
4	13	Implement the recommendation of the EPA's Information Security Task Force to manage annual security assessments, and include steps to oversee assessments to be conducted under a centralized contract or interagency agreement.	O	Chief Information Officer	9/30/16		
5	13	Implement the recommendation of the EPA's Information Security Task Force to manage the vulnerability management program.	O	Chief Information Officer	9/30/17		

[1] O = Recommendation is open with agreed-to corrective actions pending.
C = Recommendation is closed with all agreed-to actions completed.
U = Recommendation is unresolved with resolution efforts in progress.

Agency Response to Draft Report

July 23, 2015

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY14-0155 "Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance," dated June 5, 2015

FROM: Ann Dunkin
Chief information Officer

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations for the draft report "Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance (OA-FY14-0155)." Attached are two tables that incorporate comments from all EPA Program Offices that are responsible for recommendations in this audit. The first table addresses comments on specific recommendations and 'the second table contains general comments on the draft report.

AGENCY 'S OVERALL POSITION: Please note that EPA is recommending that OEI take the lead on Recommendations 3 - 6 instead of individual EPA offices. This will allow the Agency to develop a consistent approach that applies to all EPA organizations and is consistent with the recommendation by the EPA Information Security Task Force.

If you have any questions regarding this response, please contact OEI's Audit Follow-up Coordinator, Judi Maguire at maguire. judi@epa.gov or (202)564-7422.

Attachments

cc: Rudy Brevard
Kevin Christensen
Bettye Bell-Daniel
David Bloom
Janet McCabe
Karl Brooks

Thomas Burke
Judi Maguire
Maureen Hingeley
Glen Cuscino
Nicholas Grzegozewski
Brandon McDowell
Lorna Washington
Heather Cursio
Kevin Donovan
Renee Gutshall
Brenda Young

Combined Recommendations and Corrective Actions			
	OIG Recommendation	Lead	EPA Response
1.	Update the 2015 READ data call instructions to include: • A description of contractor systems that is consistent with the SLCM procedure and include a description of any other services or applications that should be included in READ (e.g., Google Apps, LexisNexis, etc.). • Language from the SLCM procedure that outlines the steps for updating the READ database for contractor systems during all applicable phases of the system life cycle. • Instructions that request a recertification that offices have verified that all contractor systems that meet the criteria within the guidance are in READ and system records are up-to-date.	OEI	**Response:** The 2015 READ Data Call included the criteria for registering a record in READ. These criteria identify systems owned by other organizations but used by EPA (which would include, with the third bullet, those systems identified in the IG report as "contractor systems"). The READ Data Call also requires each AA-ship and Region to report its completion of the READ Data Call. "READ Inclusion Criteria: READ catalogs systems and models to help the Agency, and the individual regions and program offices, improve information management, comply with internal and external data calls, avoid duplication, and meet various planning and business needs. EPA's Enterprise Architecture (EA) Policy and System Lifecycle Management (SLCM) Procedure both require registering IT systems in READ. These broad objectives require READ to be comprehensive and inclusive. A system or model should have a record in READ if it: • Has been developed or maintained using extramural dollars; or • Has been developed in-house, and used by 10 or more employees; or • Has been developed by another organization but supports EPA operations and contains EPA information (e.g., a financial system managed by another federal agency but used for internal EPA purposes); or • Contains Controlled Unclassified Information (CUI)* such as trade secret information or personally identifiable information (PII); or • Is an information resource the program office or region deems important for tracking. Please be aware that externally hosted systems (including cloud-based services) should be registered in READ. Similarly, as required by the SLCM Procedure, please register a system in READ at the Definition phase with updates to the READ record at each subsequent phase of the lifecycle." The first sub-recommendation includes a reference to services. READ should be in the catalog of systems. IT services are cataloged in EPA's Reusable Component Services (RCS). IT services are functional processes, such as Web services, that enable systems to operate and exchange information. As part of EPA's recently signed Environmental Information Management Policy (EIMP), there will be a Cataloging Procedure, which will instruct EPA programs to catalog systems in READ and to catalog IT services in the Reusable Component Services (RCS). A better sub-recommendation therefore would be: "Update the 2015 READ data call instructions to include: Language that instructs programs to register systems developed externally but used internally, consistent with the System Life Cycle Management Procedure."

2	Designate a position title in writing to be responsible for entering and maintaining the Human Resources Line of Business project components' information within READ, throughout the systems' life cycles.	OCFO, OEI	**OCFO Response:** OCFO/OFS has identified that all associated components of HRLoB included in the report: IBC, IBC Data Mart, FPPS, WTTS, EODS and other components are in READ. The entry is complete and is maintained by OHR who serves as the owner. **OEI Response:** The correct position title to use is Primary Information Resource Steward, which is the individual who is responsible for managing a READ record. Designating the Primary Information Resource Steward(s) for the READ records for the systems that comprise the Human Resources Line of Business is the responsibility of OARM, which oversees those systems. A more appropriate recommendation, which is supported by OARM, OCFO, and OEI is: We recommend that the OARM-ITD Director designate responsible individual(s) to be the Primary Information Resource Steward(s) for the READ records for the systems that comprise the Human Resources Line of Business, throughout the systems' life cycles."
3	Develop and implement a process to ensure that internal control reviews performed by contractors for iComplaints and other contractor systems owned or operated on behalf of the Office of the Administrator are requested and reviewed annually to ensure compliance with federal and agency information security requirements.	OEI	**Response** **Corrective Actions** 1. The SAISO will implement the previously approved EPA Information Security Task Force recommendation for implementing role based training and credentialing programs. Contractor oversight training will be included as part of the programs. The training and credentialing requirements for Information Security Officers are scheduled to be implemented by 30 Sep 2016. 2. The SAISO will implement the recommendation of EPA's Information Security Task Force to manage annual security assessments. The SAISO will oversee assessments to be conducted under a centralized contract or interagency agreement to be established by OEI no later than September 30, 2016. The SAISO will implement the recommendation of EPA's Information Security Task to manage the vulnerability management program.
4	Develop and implement a process to ensure that contractors for Energy Star and other contractor systems owned or operated on behalf of the Office of the Air and Radiation are implementing all federal and agency information security policies and procedures.	OEI	**Response** **Corrective Actions** 1. The SAISO will implement the previously approved EPA Information Security Task Force recommendation for implementing role based training and credentialing programs. Contractor oversight training will be included as part of the programs. The training and credentialing requirements for Information Security Officers are scheduled to be implemented by 30 Sep 2016. 2. The SAISO will implement the recommendation of EPA's Information Security Task Force to manage annual security assessments. The SAISO will oversee assessments to be conducted under a centralized contract or interagency agreement to be established by OEI no later than September 30, 2016. The SAISO will implement the recommendation of EPA's Information Security Task to manage the vulnerability management program.

5	Develop and implement a process to ensure contractors for the PRIS and other contractor systems owned or operated on behalf of the Office Research and Development are implementing all federal and agency information security policies and procedures.	OEI	**Response** **Corrective Actions** 1. The SAISO will implement the previously approved EPA Information Security Task Force recommendation for implementing role based training and credentialing programs. Contractor oversight training will be included as part of the programs. The training and credentialing requirements for Information Security Officers are scheduled to be implemented by 30 Sep 2016. 2. The SAISO will implement the recommendation of EPA's Information Security Task Force to manage annual security assessments. The SAISO will oversee assessments to be conducted under a centralized contract or interagency agreement to be established by OEI no later than September 30, 2016. The SAISO will implement the recommendation of EPA's Information Security Task to manage the vulnerability management program.
6	Develop and implement a training program to educate program and regional offices about their oversight responsibilities for federal and agency information security requirements for contractor systems. The training program should include developing a roster of personnel who require training, and implementing a process to ensure personnel complete the training.	OEI	**Response** **Corrective Actions** 1. The SAISO will implement the previously approved EPA Information Security Task Force recommendation for implementing role based training and credentialing programs. Contractor oversight training will be included as part of the programs. The training and credentialing requirements for Information Security Officers are scheduled to be implemented by 30 Sep 2016. 2. The SAISO will implement the recommendation of EPA's Information Security Task Force to manage annual security assessments. The SAISO will oversee assessments to be conducted under a centralized contract or interagency agreement to be established by OEI no later than September 30, 2016. The SAISO will implement the recommendation of EPA's Information Security Task to manage the vulnerability management program.

Appendix B

OIG Revised Recommendations and EPA's Agreed-to Corrective Action Plan

OIG Revised Recommendation	EPA Response and Milestone
We recommend that the Chief Information Officer: 1. Update the 2015 READ data call instructions to include: • Language that instructs programs to register systems developed externally but used internally, consistent with the System Life Cycle Management Procedure. • Language from the SLCM procedure that outlines the steps for updating the READ database for contractor systems during all applicable phases of the system life cycle. • Instructions that request a recertification that offices have verified that all contractor systems that meet the criteria within the guidance are in READ and system records are up-to-date.	We have met Recommendation 1 by issuing the 2015 READ Data Call. In this data call, we added the criteria for including a record in READ. These criteria contain language that states that systems developed externally but used internally should be registered in READ and that a system should be registered and that record maintained throughout its lifecycle as directed in the SLCM. The data call further directed EPA programs to report to OEI when their portfolio of READ records have been updated. **Completed**: May 27, 2015
We recommend that the Assistant Administrator for Administration and Resources Management: 2. Designate responsible individual(s) to be the Primary Information Resource Steward(s) for the READ records for the systems that comprise the Human Resources Line of Business Initiative, throughout the systems' life cycles.	The systems that comprise the HR Line of Business are now registered in READ, with a Primary Information Resource Steward designated for each **Completed:** February 27, 2015.
The OIG concurs with the corrective action plan and milestone dates and proposes the following revised recommendations: We recommend that the Chief Information Officer: 3. Implement the previously approved EPA Information Security Task Force recommendation for implementing role-based training and credentialing programs, and include contractor oversight training as part of the programs. 4. Implement the recommendation of the EPA's Information Security Task Force to manage annual security assessments, and include steps to oversee assessments to be conducted under a centralized contract or interagency agreement. 5. Implement the recommendation of the EPA's Information Security Task Force to manage the vulnerability management program.	Milestone for Recommendation 3: September 30, 2016 Milestone for Recommendation 4: September 30, 2016 Milestone for Recommendation 5: September 30, 2017

Appendix C

Specific Elements of Criteria Used for Reviewing Security Controls for Selected Systems

Agency criteria	Procedure control area tested	Specific element(s) of control area tested
CIO-2150.3-P-08.1, *Information Security - Interim Incident Response Procedures*, v3.1, July 19, 2012	IR-5 – Incident Monitoring	a. Information system security incidents must be tracked and documented.
	IR-8 – Incident Response Plan	a. An Incident Response Plan must be developed that: i. Provides the organization with a roadmap for implementing its incident response capability. ii. Describes the structure and organization of the incident response capability. iii. Provides a high-level approach for how the incident response capability fits into the overall organization. iv. Meets the unique requirements of the organization, which relate to mission, size, structure and functions. v. Defines reportable incidents. vi. Provides metrics for measuring the incident response capability within the organization. vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability. viii. Is reviewed and approved by designated officials within the organization.
CIO-2150.3-P-04.1, *Information Security – Interim Security Assessment and Authorization Procedures*, v2, July 16, 2012	CA-2, Security Assessment and Authorization Control family identified by NIST 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations	a. A Security Assessment Plan that describes the scope of the assessment must be developed to include: i. The security controls and control enhancements under assessment. ii. The assessment procedures to be used to determine security control effectiveness. iii. The assessment environment, assessment team, and assessment roles and responsibilities. e. A Security Assessment Report must be developed to document the results of the assessment. f. The results of the security control assessment must be provided, in writing, to the authorizing official or the authorizing official's designated representative. l. When the potential impact on agency operations, agency assets, individuals, other organizations, and the nation is low (e.g., low FIPS 199 security categorization), a self-assessment activity is an acceptable and cost-effective mechanism to fulfill the security assessment requirement. (For information systems FIPS 199 categorized as low) n. NIST SP 800-53A, Revision 1 must be used as guidance for security control assessments.

Source: OIG compiled.

Appendix D

Internal EPA Contractor-Supported Systems Not Reported in READ

EPA Office	Number	System name
Office of Administration and Resources Management	1	Personnel Security System (PSS)
Office of Environmental Information	2	TDX
	3	TRI FAST
Office of Research and Development	4	ORD Enterprise General Support Systems (GSS)
	5	Atmospheric Modeling clusters
	6	SuperMuse
	7	Corvallis and Newport Facilities Server
	8	Duluth METASYS Network
	9	Facility LAN
	10	Chemistry LAN
	11	ERD BACnet Building Automation Server
	12	ILCO Millennium- access card system
	13	Sting Alarm Systems- Video surveillance
	14	Unauthorized Commitments Training/NERL
	15	Oracle Grid Control
	16	ORD@Work
	17	ORD Application Inventory
	18	Bugbase
	19	Consolidated Human Activity Database Explorer version 2 (CHADexplorer version 2)
	20	HEASD Log
	21	Barometric Pressure
	22	Centroid
	23	Decision Analysis for a Sustainable Environment, Economy, and Society
	24	EPA MARKAL Databases (EPAUS9r_12_v1.2, EPANMD_12_v1.2)
	25	Health and Safety Plan
	26	Health and Safety Plan Online Creator Assistant
	27	i-SVOC—a simulation program for indoor SVOCs
	28	Leaching Environmental Assessment Framework

EPA Office	Number	System name
	29	Program for Assisting the Replacement of Industrial Solvents
Office of Research and Development	30	Universal Industrial Sector Integrated Solutions
	31	Petroleum Hydrocarbon Source Term Model for Vapor Intrusion and Ground Water Contamination
	32	ACE
	33	Acute & Chronic Toxicity Database
	34	Library AED Bibliography System
	35	AED Records Management Database
	36	AquaChronTox
	37	GED - Acute Toxicity Data
	38	GED - Benthic Data
	39	GED - Environmental Bibliography
	40	GED - Committees
	41	Detroit River MB-IPP
	42	Ecosystem Goods and Services, Public Health and Well-Being Browser
	43	Environmental Management System EMS / Doc Lib
	44	EPA H2O
	45	Environmental Quality Index
	46	GED Facilities
	47	Final Ecosystem Goods and Services Classification System
	48	Fox River/Green Bay
	49	FTOX
	50	Gulf Ecology Model (GEM) and Gulf of Mexico Dissolved Oxygen Model (GoMDOM)
	51	Gulf of Mexico Dissolved Oxygen Model
	52	Great Lakes Nutrient Loading
	53	Hazardous Waste request Form
	54	Human Well-Being Index
	55	HYGIEIA
	56	Lake Michigan Atrazine
	57	Lake Michigan Nutrients
	58	Lake Michigan PCB
	59	LIBRARY
	60	Nearshore database
	61	Pacific Coast Ecosystem Information System
	62	Population Matrix
	63	ReefLink
	64	Respiratory Physiology
	65	Simulation of Metacommunities of Riverine Fishes

EPA Office	Number	System name
	66	Technical Assistance Information System
Office of Research and Development	67	Tampa Bay Ecosystem Services Demonstration Project Digital Atlas
	68	TERS Request System
	69	Upper Midwest Landscape
	70	VELMA ecohydrological model and decision support framework
	71	VIDEOPROFILES
	72	Athens ERD Phone List
	73	Athens Laboratory Corrective Action Tracking System
	74	ORMA - Extramural RMSS Tracking System
Region 5	75	Planning & Budget Information Tracking System (PBITS)
Region 6	76	Zazio Versatile Enterprise (Records Center)
	77	Smart Track (Mail/Supply Room Tracking)
	78	CLP Tracker
	79	ESRI ArcGIS (License Subscription)
	80	ETM (Warehouse Management Tool - License Subscription)
Region 7	81	CERETS - Comprehensive Emergency Response Equipment Tracking System

Source: OIG compiled.

Appendix E

Distribution

Office of the Administrator
Chief Information Officer
Assistant Administrator for 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 and Deputy Chief Information Officer, Office of Environmental Information
Principal Deputy Assistant Administrator, Office of Administration and Resources Management
Senior Agency Information Security Officer, Office of Environmental Information
Director, Office of Policy and Resource Management, Office of Administration and Resources Management
Deputy Director, Office of Policy and Resource Management, Office of Administration and Resources Management
Audit Follow-Up Coordinator, Office of Environmental Information
Audit Follow-Up Coordinator, Office of Administration and Resources Management