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

JAN 04 2016

THE INSPECTOR GENERAL

MEMORANDUM

SUBJECT: Analysis of Office of Environmental Information Response to Office of Inspector General Report No. 15-P-0290, *Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance*,
Issued September 21, 2015

FROM: Arthur A. Elkins Jr.

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

Thank you for providing your comments to our final report and noting areas your office believes are inaccurate. We agree with the purpose of the Registry of the Environmental Applications and Data Warehouse (READ) and its importance as a tool for improving the U.S. Environmental Protection Agency's (EPA's) ability to manage its information resources. However, we stated that the EPA lacked a complete inventory of contractor systems. By not assessing the operating effectiveness of a contractor's information system security control environment, the EPA risks the ability to protect its information resources and data from undue harm. During our audit, many offices expressed confusion as to what information should be recorded in READ. In response to those concerns, your office issued updated instructions to program and regional offices to clarify what information should be recorded in READ. We agree with the corrective actions the agency is taking to address the final report recommendations.

Overall, we believe the concerns you have highlighted do not constitute a need for us to make any changes to our final report. Attached is your response to our report in which we inserted an OIG analysis in specified areas. Your response will be posted on the Office of Inspector General's public website, along with this memorandum commenting on your response.

We will post this memorandum to our website at www.epa.gov/oig.

Attachment

Attachment

OIG Responses to OEI Comments to OIG Final Report

MEMORANDUM

SUBJECT: Response to Office of Inspector General Final Report No. 15-P-0290 "Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance," dated September 20, 2015

FROM: Ann Dunkin /s/
Chief Information Officer

TO: Arthur A. Elkins Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations for the final report "Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance (15-P-0290)."

AGENCY'S OVERALL POSITION: OEI has the following comments on the final report.

- The drafts of this report included tables containing lists of applications that the IG determined were not in READ. The information in these tables was obtained from EPA Regional and Program Offices. Although several EPA Program Offices and Regions provided feedback that some of this information was incorrect, the subsequent draft and final report did not reflect this information. For example, Region 6 provided feedback that four of the seven applications listed in the tables were reported to the IG in error and should not have records in READ, but these applications continued to be listed in the later draft and final report. In addition, the final report includes ORD applications even though the IG is aware that ORD maintains a separate database and that an API is being written to synchronize the ORD database with READ. As a result of the above information, the number of applications listed as missing from READ is overstated in this report.

  OIG Response 1: *During our audit, regional and program office personnel were uncertain on which contractor systems should be recorded in the Registry of the Environmental Applications and Data Warehouse (READ). According to the U.S. Environmental Protection Agency's (EPA's) Chief Information Officer Transmittal Number 12-004, System Life Cycle Management (SLCM) Procedure, all EPA information technology systems and application projects, including custom developed, commercial-off-the-shelf, and government-off-the-shelf projects should be entered and updated in the agency's official system inventory registry known as READ. Throughout the audit, we received feedback from EPA offices regarding their belief why a particular contractor system should not be in READ and where appropriate, we adjusted the report tables.*
  OIG Response 2: *In response to our request for information, Region 6 provided us a listing of 12 contractor systems they believed should be recorded in READ. Similar to other offices, Region 6 inquired whether a system should be recorded in READ and the*

regional personnel stipulated they were not sure of the correct answer. Region 6 personnel also questioned whether the Office of Environmental Information (OEI) should enter the READ information for some of their systems that are agencywide applications. Working with the region, we were able to narrow their list down to six systems that were not recorded in READ. The final report lists two systems (License Subscriptions) that Region 6 believed to be agencywide systems that we identified as not being recorded in READ. We listed these systems under Region 6 because the regional personnel identified themselves as the location using the systems in question. We brought this issue to the attention of OEI personnel and we believe it is incumbent upon management to ensure these systems are recorded in READ under the correct EPA office.

OIG Response 3: *During our audit, Office of Research and Development (ORD) personnel indicated they were conducting an internal data call of ORD's systems which would be use to populate a new database; however, the database was under development and no timeframe was provided on when the database would be fully operational. Therefore, we listed ORD's contractor systems in the final report, because these systems were not entered in READ as required by the EPA's SLCM procedure.*

- We would like to clarify the information about the ISTF included in the IG's final report. The report includes recommendations that the Agency implement the approved ISTF recommendations. We agree with that recommendation. However, we are concerned that the recommendation could be misunderstood by someone reading the report to suggest that the EPA has not been working to implement those recommendations. To provide additional context, we wish to make it clear that the Agency initiated work on the ISTF recommendations immediately after they were approved. Staff continue to work diligently to complete the recommended actions.

OIG Response 4: *The OIG revised the draft report's original recommendations to reflect the efforts OEI made in developing the Information Security Task Force (ISTF) action plan. We replaced our original four draft report recommendations with three proposed alternative recommendations that OEI believed would address our concerns. We reviewed the ISTF action plan and agreed that once OEI completed the specified corrective actions, the ISTF recommended actions would address our concern. However, the plan submitted for our review lacked milestone dates for when the EPA would complete the corrective actions for the areas of our concern. Upon subsequent discussions with OEI representatives, we were able to obtain projected dates when the EPA would complete the corrective actions for the areas where we had findings and expressed concerns.*

- Regarding the statement on page 5 and the conclusion on page 8 that failing to list systems in READ creates a security risk, OEI wants to emphasize that the purpose of READ is not related to security. Xacta is used to manage system security information. In Xacta a "system" represents a grouping and tracking of assets from an information security perspective. READ is an inventory of applications, data warehouses and models where any one of which may not in and of itself be identified as a system. There is not always a one-to-one correspondence of application in READ to systems in Xacta. Therefore READ is not a tool used to manage and track system security. There are other processes in place to support the use of Xacta to manage system security.

OIG Response 5: *OEI describes READ as the authoritative source of information about EPA information resources. OEI further states that (1) READ is an important tool for* *improving the EPA's ability to manage its information resources and (2) having an accurate inventory of which information resources exist at the EPA is a first step in effective management. We agree with OEI's position on the importance of READ and the effectiveness of having an accurate system inventory. Having an accurate system inventory, in order to effectively monitor security of the EPA's information resources, has been a long-standing concern for our office. As noted in OIG Report No. 10-P-0146, Improvements Needed in Key EPA Information System Security Practices, we recommended that the EPA implement a process to perform a periodic reconciliation of the agency system used to track information security (formerly ASSERT and currently XACTA) and READ to ensure the agency has effective oversight of all systems that require monitoring. Your office agreed with the recommendation and specified that your office completed an analysis of the data in both systems in May 2011 and would annually, in May, conduct a cross-walk between the records in the system used to manage information system security with the records in READ. We continue to believe that without knowing what systems require protecting, the EPA is unable to make sound technology investment decisions to effectively protect its network or the information resources dependent upon it.*

- In addition to believing there is no connection between the inclusion of a system in READ and security, the Agency continues to have concerns about the methodology used to apply a cost to a possible breach of PRPIS and iSTAR. We appreciate that the IG included the sources of its breach cost estimates in the final report. We reviewed the latest Ponemon institute study (the IG's source was the 2013 study), a summary of which (and link to the full report) can be found at this URL: http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html. We believe that there is insufficient data in the publicly available materials to understand the methodology and, therefore, use it to estimate the cost of a breach.

  If one reads the US specific report, there is a statement that "In contrast, public sector (government), hospitality and research have a per capita cost well below the overall mean value." The report goes on to provide a table that shows the average cost of a public sector data breach to be $73. This number is an average and does not differentiate between breaches that include SPII, PII or public data. Therefore, more information would be required to estimate the cost of a breach of the systems listed in the IG's report using the Ponemon methodology.

  OIG Response 6: *We began this audit in February 2014 and provided the EPA with our discussion draft report in January 2015, approximately 5-months prior to the Ponemon Institute issuing the 2015 data breach report. During our audit, we used the 2013 Ponemon data breach report, which was the current report available during the field work portion of the audit. Our subsequent comparison of the two reports disclosed that the Ponemon Institute used a different methodology, in 2015, to calculate the cost of a data breach than was used in the 2013 report. As you noted in your response, the public version of the 2015 Ponemon Institute data breach report does not provide sufficient details to understand the methodology used for calculating a data breach and we are unable to determine whether all the same cost factors used in 2013 were used in the 2015 report. The 2013 Ponemon report provides sufficient details on the methodology used to calculate the cost of a data breach and we made this information available to your staff. Based on 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 (using $142 per record for the Peer Reviewer Information System and $100 per record for the iStar* *system). When we consider just the $73 cost per record listed in the 2015 Ponemon report, without considering any other cost factors, a breach would cost EPA $8.9 million if all the records within the two systems were compromised. This is well within our original projected estimates and the cost difference is not material to the overall finding that data breaches could have a substantial impact to the EPA's budget. As noted in the 2013 report, the Ponemon Institute projected $188 as the average cost per record fora data breach. We adjusted this figure considerably to take into consideration key factors, such as a formal incident response plan or recurring security assessment testing of the system's security posture which we noted existed for the systems under review. We also factored out the cost for identity protection services since neither system in our review contained financial information. We believe we used a sound methodology, for calculating the potential cost of a data breach, which provides a reasonable basis for our conclusions.*

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