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

NOV 20 2015

OFFICE OF
ENVIRONMENTAL INFORMATION

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 Carol [illegible]
Chief Information Officer for

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.

- 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.

- 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.

- 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.

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.

cc: Rudy Brevard
Bettye Bell-Daniel
Judi Maguire
Nicholas Grzegozewski
Kevin Donovan
Renee Gutshall
Brenda Young