Appendix D

OCIO Response to Draft Report

U.S. Department of Labor

Office of the Assistant Secretary for Administration and Management
Washington, D.C. 20210

MAR 27 2015

MEMORANDUM FOR ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: DAWN M. LEAF
Chief Information Officer

SUBJECT: Management Response to the Office of the Inspector General Fiscal Year 2015 Draft Audit Report Entitled: Cyber Security Program Improvements Are Needed to Better Secure DOL's Major Information Systems, Report No. 23-15-001-07-725

This memorandum responds to the above-referenced Fiscal Year 2015 draft audit report dated March 18, 2015. The Office of Inspector (OIG) performed audit testing of 15 Department of Labor (DOL) major information systems and issued 75 Statements of Facts to the System Owners. As a result of combining the system specific deficiencies, the OIG outlined four DOL entity-wide "significant deficiencies" for Third-Party Oversight/Monitoring, Vulnerability and Configuration Management, Contingency Planning/Disaster Recovery and Access Management resulting in the issuance of four recommendations. Although not considered significant deficiencies, the OIG also identified other Information Technology (IT) security deficiencies for IT Asset Management and Incident Response resulting in the issuance of one recommendation.

The Office of the Chief Information Officer (OCIO) appreciates the efforts of the OIG, and takes very seriously its responsibility to safeguard DOL IT systems and information. Management agrees that improvements are needed to better secure DOL's major information systems and will ensure corrective actions are taken as appropriate. In management's view, the items outlined in the report as contributing to the significant deficiency for Contingency Planning does not provide the requisite linkage between the findings and risks outlined in the report that could realistically be expected to rise to the level of significance at a Department-level. Management's response to the recommendation outlined in the report follows.

Recommendation 1
We recommend the Chief Information Officer establish third-party oversight/monitoring processes and tools that guide information system owners on how to better monitor third-party service providers' effectiveness in implementing NIST information security requirements and Administration priorities.

- *Response:* The DOL Computer Security Handbook, Volume 15, section 3.2.5, establishes the requirements for monitoring third-party compliance with the Department's system security policies and standards. In an effort to strengthen its ability to monitor third-party

providers, the Department drafted a Third-party Security Monitoring Guide for DOL Agencies to use for monitoring third-party managed IT systems from an IT security standpoint. This Guide includes a checklist that Agencies may use to assess the level of compliance of third-party service providers employed by DOL. This guide is planned to be finalized and issued in FY15 Q3.

Please reference Plan of Action and Milestones ID #20790 for more details. Management considers this recommendation resolved with closure dependent on the completion of the actions outlined above.

Recommendation 2:
We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of the Department's cyber security program related to the Vulnerability and Configuration Management Significant Deficiency.

Response: The DOL Information Security Continuous Monitoring (ISCM) program enables the OCIO to collect enterprise information using automated tools to determine information system compliance with vulnerability, configuration and asset inventory management. The automated tools used in support of the ISCM program also provide Agencies access and views in near real-time data of information systems. To maximize the limited financial resources available to Agencies for their IT security projects following the DOL-wide IT budget cuts in FY 2014, the OCIO established priority security metrics to address the issues contributing to the highest risk areas across the Department. OCIO instituted quarterly security dashboards to monitor Agencies progress in achieving the DOL security priority metrics. As a result of the ISCM ongoing efforts, DOL realized a 60% decrease in the number of information system vulnerabilities, and a 49% decrease in the number of outstanding security patches. These outcomes indicate the OCIO oversight program is operating effectively. Building on this progress, in FY 2015, the OCIO will deploy additional automated continuous monitoring tools and will continue working with Agencies to strengthen their vulnerability and configuration management control processes and procedures.

Management considers this recommendation closed pending OIG validation.

Recommendation 3:
We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of the Department's cyber security program related to Contingency Planning / Disaster Recovery.

Response: OCIO performs oversight reviews of DOL Agencies' system Contingency Planning and testing activities. Although the OIG identified deficiencies in a small percentage of DOL Major Information System sub-components, all systems have Contingency Plans in place that are appropriate for the restoration of the business functions for which they support. While all DOL system Contingency Plans have been tested within the last two years, due to budget constraints, some of the planned testing exercises were delayed and not considered to have been tested within a 12 month period. In FY 2015, the OCIO will work with DOL Agencies to review their

Contingency Planning processes, including testing, to ensure they perform full testing of their systems in an appropriate timeframe and as permitted by IT budgets.

Management considers this recommendation closed and no further action will be taken.

Recommendation 4:
We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of the Department's cyber security program related to Access Management.

Response: The OCIO will increase communication with DOL Agencies to ensure they give priority attention to prioritize and complete the corrective actions required to address the identified access management issues and will monitor Agency progress on addressing these deficiencies. We will also continue to explore technical solutions to address access and account management issues. Additionally, due to the DOL IT budget cuts, the Identity and Access Management (IAM) program was not fully funded. While the OCIO made considerable progress in deploying IAM Phase 1: Deploying Logical Access Control infrastructure components to over 95% of the Department's environment enabling users to leverage their Personal Identity and Verification card for network access, the Department did not receive funding to implement IAM Phase II: Identity Management System. As a result, full IAM implementation has been delayed until the Q1 FY 2016, contingent upon budget approval.

Please reference Plan of Action and Milestones ID #18678 for more details. Management considers this recommendation resolved with closure dependent on the completion of the actions outlined above.

Recommendation 5:
We recommend the Chief Information Officer conducts better oversight of DOL's information technology asset and incident response management areas to ensure full and effective implementation of the security controls identified in Section B of the draft report.

Response: Although there is no federal mandate for an enterprise-wide automated IT Asset Management System for moderate systems, NIST 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, does require federal organizations to maintain information system inventories to the extent feasible. To that end, the Department implemented a two-fold system asset inventory process. This process includes Agencies using CSAM to document their information system inventory annually and the use of an automated enterprise monitoring tool to automate other aspects of DOL's asset inventory process. OCIO management will continue to research methods and technologies that will augment the current processes for DOL's full IT assets tracking and management.

The DOL Computer Security Incident Response Capability (DOLCSIRC) works diligently with DOL Agencies to ensure all incidents are handled and reported in accordance with federal and Departmental requirements. DOLCSIRC coordinated a total of 229 incidents for the Agencies audited in FY 2014. Although 3% of the 229 incidents were found to have been reported outside of the reporting timeframes, all incident handling procedures were completed. Recognizing the importance of timely reporting, the OCIO provided several incident response training sessions in