APPENDIX B: AGENCY'S RESPONSE TO THE REPORT

U.S. Department of Labor

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

MEMORANDUM FOR: ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA Digitally signed by GUNDEEP AHLUWALIA Date: 2019.10.24 17:06:09 -04'00'

SUBJECT: Management Response to the DRAFT REPORT – Stronger Controls Needed Over Web Application Security, Draft Report No. 23-20-001-07-725

This memorandum addresses the above-referenced DRAFT REPORT – *23-20-001-07-725 Stronger Controls Needed Over Web Application Security* issued to the DOL Chief Information Officer (CIO) on October 3, 2019, for management's review and response.

DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas to improve security for our information systems and data. OCIO management concurs that at the completion of the OIG Field Work in 2016 the Notice of Finding and Recommendation was valid. However, since that time, the DOL's IT environment has significantly changed and the security posture matured. OCIO contends that the changes and improvements affect the conditions related to this NFR to the point that they can be closed. Those changes and improvements include:

1. As part of the continuous monitoring program to address security vulnerabilities relating to public facing websites, DOL's internet perimeter is scanned by DHS. These scans capture and provide a list of all DOL websites. DHS also provides OCIO weekly cyber hygiene reports which indicate any related identified vulnerabilities. Agencies are required to reconcile their web sites to the list provided by the DHS. Identified vulnerabilities (to systems containing sensitive and non-sensitive information) are remediated accordingly. This process provides assurance that DOL's websites and by extension web applications are adequately secured and in alignment with the DHS reports.
    - See attached DHS Cyber Hygiene Assessment Report (cyhy-DOL-2019-10-06T231652+0000.pdf)
    - See attached DOLCSIRC alert to address the weaknesses (DOLCSIRC-N-20-006 (DHS Cyber Hygiene Scan-results) Update 1 TLP AMBER.msg)

2. The information security continuous monitoring (ISCM) approach has undergone several revisions with much emphasis on POA&M management within the Department's information security and risk management program documentation. The Department's POA&M management process (POA&M Management Guide v1.2) has been enhanced to ensure corrective actions and time frames are implemented according to policy. This process has increased the review frequency, realigned the review to include qualitative and quantitative performance measures of POA&M activities and use the information to make appropriate adjustments as needed, follow up and reporting to management.
    - See attached POA&M Management Guide v1.2

3. As it relates to establish and verify the implementation of Department-wide policies and procedures specific to associated risks to web applications, securing web servers, and web application programming; while the policies do not explicitly reference "web applications", the Computer Security Handbook Edition 5 (CSH 5) volumes below are among the Department's policies and procedures that address hardening web server operating environment:
    - Access Control Protection Policy, Procedure and Standards, Version 1.1 (Last Update 8/14/2018)
    - Audit and Accountability Policy, Procedures, and Standards, Version 1.0, (Last update 3/31/2016)
    - Identification and Authentication Policy, Procedures, and Standards, Version 1.0, (Last Update 6/5/2018)
    - Configuration Management Policy, Procedures, and Standards, Version 1.0, (Last Update 8/27/2018)

    In particular, CSH Volume 5 – Configuration Management, section 3.1.5 states "***DOL's required minimum standards on configuring settings for information technology products are as follows:…*** *FISMA, section 3544(b)(2)(D)(iii), requires each federal agency to develop "minimally acceptable security configuration requirements" and ensure compliance with them. All security configuration standards issued as part of this volume comply with FISMA and the Department of Labor Manual Series (DLMS) Chapter 9 Section 400 (407)(A)(2)(b) and are based on the criteria listed below:…*

    c. *In the absence of NIST guidance to address a specific technology, common secure configurations (also referred to as a NIST approved security configuration checklist (such as but not limited to the United States Government Configuration Baseline (USGCB), Security Content Automation Protocol (SCAP), Common Configuration Enumeration (CCE)), lockdown and hardening guides, security reference guides, security technical implementation guides) must be utilized."*

    Management contends that this policy applies to and addresses associated risks to all services including websites and web applications.

OCIO believes that all the above actions are sufficient to close the recommendations. In addition, Management recommends the OIG revise the opening statement "The Department of Labor (DOL) managed 72 publicly accessible web applications as of March 2019", to reflect that this was the state of the inventory as of 2016 not 2019.

We appreciate the opportunity to provide input. If you have any questions, please contact me directly at (202)-693-4446 or have your staff contact Paul Blahusch, Chief Information Security Officer, at Blahusch.Paul.E@dol.gov or (202) 693-1567.

cc: Bryan Slater, Assistant Secretary for Administration and Management
Al Stewart, Deputy Assistant Secretary for Operations
Paul Blahusch, Chief Information Security Officer (CISO)
Scott Davis, Deputy Chief Information Security Officer (CISO) D/CISO
Muhammad Butt, Division Director, Information Security Policy & Planning (ISSP)