MANAGEMENT'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

12/13/2019

SUBJECT: Management Response to the DRAFT REPORT – FY19 FISMA DOL Information Security Report: Implementation of Security Tools Hindered by Insufficient Planning;
Report No. 23-20-002-07-725

The Office of the Assistant Secretary for Administration and Management (OASAM), Office of the Chief Information Officer (OCIO) – hereafter referred to as *management* – remains committed to ensuring the Department of Labor (Department or DOL) implements an effective security program to protect its information and information systems. The independent evaluations performed under the direction of the Office of the Inspector General (OIG) are a key component in measuring this program's effectiveness. As such, management appreciates this evaluation and the opportunity to review and comment on the Draft Report titled *FY19 FISMA DOL Information Security Report: Implementation of Security Tools Hindered by Insufficient Planning*.

However, management has a number of concerns with the report that, if addressed, we believe will improve the report's accuracy and usefulness. These concerns are:

Self-Assessment

Management believes the criticism of the accuracy of our self-assessment is undeserved. As a deliverable to the OIG evaluation team, OCIO performed a self-assessment of our cybersecurity posture using a questionnaire provided by the OIG team that was derived from the federal-wide IG FISMA reporting template. The template asked OCIO to rate our program level of maturity from 1 (ad-hoc) to 5 (optimized) in 59 specific control areas. The template provided high-level definitions of the maturity level in each area rated. As stated in the report (page 12) – "Level 4, Managed and Measureable, is considered to be an effective level of security." Anything below that level is considered "Not Effective."

Based on our experience from previous years' evaluations, we believed that the OIG team would test and rate our maturity no higher than what we self-assessed. This belief is supported by the fact that in previous years where we self-assessed at Level-3 "Consistently Implemented," in no instances did we receive a rating higher than Level-3 for any control. Therefore, to be considered for Level-4 (i.e. "Effective"), we aggressively sought out areas

where we felt we could reasonably be considered for a Level-4 rating – in short, we wanted to be evaluated at a higher standard to see how we measured up, and to see in what areas we fell short. And, in fact, we measured up pretty well – improving in 21 of 59 individual controls, including 16 rated as Level-4, and with the overall Protect control area rated as Level-4. These are the highest ratings DOL had ever achieved.

Also, as mentioned above, we based our self-assessment on the template provided by the OIG team at the beginning of the audit. Months later, in discussions with the OIG team over the results of their assessment, we learned there was a more detailed evaluation guide they were using. Basically, when we performed our self-assessment we did not have complete information on the criteria against which we'd be rated. If we had this guide at the outset as a reference to perform our self-assessment, perhaps there would have been more concurrence between our ratings.

For these reasons, we believe the criticism of the accuracy of our self-assessment (i.e. self-awareness) should be removed from the overview and the cover letter.

Implementation Plans

In the overview, and again in the cover letter, it is stated that "OCIO was unable to provide timelines and plans for any of the information security tools not fully implemented, indicating the utilization of these tools was not properly managed." This is misleading as it implies that *any* security tool in OCIO not fully implemented has no plans or timelines. Rather, the assessor did not evaluate all ongoing OCIO security tool implementations, only those which management referenced in the course of the assessment. This is reflected on page 12 of the report, which reads "We requested project plans for the implementation of the tools referenced by DOL management; however, management failed to provide approved project plans that document the planned completion dates of these implementation projects." DOL has implementation plans and timelines for a number of security tools including for those addressing identity and access management, continuous monitoring, content filtering, data leak prevention, and network access control. Management believes the wording in the overview and cover letter would more accurately describe the condition found as: "For security tools referenced by management in the course of this assessment that were not fully implemented, OCIO was unable to provide timelines and plans, indicating the utilization of these tools was not properly managed."

Incident Reporting

The failure of OCIO to report incidents in a timely fashion to the United States Computer Emergency Readiness Team (US-CERT) is mentioned on pages 17, 18, 19 and 20. While management acknowledges that we did not report all incidents to US-CERT within one hour of OCIO confirming the incident, as our policies require and for which we strive to achieve, our incident tracking records show that of the 317 incidents we reported to US-CERT this year, 301 (95%) were reported within one hour. Of those not reported within the one hour, most were reported within three hours, with the longest delay being about three days. In addition, those not reported within the prescribed timeframe were quickly identified and

management took immediate corrective action. We believe when examined in total that the DOL incident reporting program, while not perfect, is certainly operating at an acceptable level and that while the few deficiencies are fairly noted, they do not rise to the level of a reportable finding.

Encryption of Data-at-Rest

On page 17 (and again on page 18) of the report, it is stated that OCIO is not meeting a requirement to encrypt data-at-rest – specifically data-at-rest on servers. Management concurs with the condition – we are not routinely encrypting data on servers; however we disagree that this is a requirement. The applicable NIST SP800-53 security control (*SC-28 PROTECTION OF INFORMATION AT REST*) requires that we employ mechanisms to protect the data, which DOL achieves through a number of physical and logical controls on servers, but does not specify encryption must be used to protect the data. In fact, encryption as a specific protection method is a *Control Enhancement* that is specifically not applicable to a moderate-rated information system such as exist in the Department. For this reason we believe references to encryption of data-at-rest as a requirement should be removed from the report.

Compensating Backup Controls

On page 20 (and again on page 21) of the report is described a condition where a routine backup operation was not functioning appropriately. The description is incorrect in stating that the cause was a "technical configuration error." The actual cause was due to a hardware failure in the backup device. Management requests that the description of the cause be corrected. In addition, we believe it is important to note that at no time was data at risk of loss, as IT personnel were quickly alerted to the condition and an alternate, compensating backup method was used until the hardware could be repaired.

Recommendations

Management concurs with the recommendations listed on pages 22-23 of the report with the following exceptions:

- Re-word recommendation #7 to make it clear that it only applies to security-related patches and updates (as opposed to functionality or performance updates) – i.e. "Design and implement controls to monitor DOL assets for missing security patches, service packs, hot fixes, and other security-related software updates that are not associated with a CVE.";
- Combine recommendations #14 and #17 as they both address training in incident reporting guidelines;
- Remove recommendation #15 because, as described above, encryption of data-at-rest on servers is not required; and
- Remove recommendation #20 because the monitoring and controls regarding backup failure notification worked as designed in the situation evaluated, and the data was backed-up using an alternate method.

Again, management appreciates the evaluation performed and values the observations and recommendations offered to improve the protections of the Department's data and information systems. We were pleased that some of our accomplishments were included in the report, such as:

- Our achieving Level 4 – Managed and Measurable in the Protect control area (page 9);
- That 21 of 59 (36%) of individual control areas showed improvement from FY18 (page 10);
- The Department's continued strides in implementing tools from the DHS Continuous Diagnostic and Mitigation program (page 12); and
- Our implementation of strong authentication methods for user access, including onboarding service accounts (page 16).

In addition, though not noted in the OIG FISMA report, DOL achieved the following positive cybersecurity results during FY19:

- Met or exceeded 8 of 10 (80%) of the President's Management Agenda Cross-Agency Priority Cybersecurity Goals;
- Maintained an overall highest rating of "Managing Risk" in the FY19 OCIO FISMA report, including improving our rating in five individual control areas;
- Closed 41 of 63 (65%) open OIG findings from previous years;
- Began implementation of an IT Shared Services initiative that will place all Department IT under the direct authority of the CIO in 2020; and
- Was recognized by the U.S. Government Accountability Office as one of 7 (of 23) Chief Financial Officers Act agencies to fully establish an agency-wide cybersecurity risk management strategy to guide the agency's risk decisions.