APPENDIX C: CIO'S RESPONSE TO THE REPORT

U.S. Department of Labor

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

1/23/2023

MEMORANDUM FOR: CAROLYN R. HANTZ
Assistant Inspector General for Audit

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA
Digitally signed by GUNDEEP AHLUWALIA
Date: 2023.01.23 16:52:35 -05'00'

SUBJECT: Management Response to the DRAFT REPORT - (Fiscal Year) *FY 2022 FISMA DOL Information Security Report: DOL's Information Security Program Not Remaining Current with Security Requirements*, Report Number: 23-23-001-07-725

This memorandum responds to the above-referenced Draft Report – (Fiscal Year) *FY 2022 FISMA DOL Information Security Report: DOL's Information Security Program Not Remaining Current with Security Requirements*, issued October 21, 2022. DOL leadership is committed to continuously strengthening DOL's cybersecurity posture. As such, DOL continues to prioritize cybersecurity as a key focus area.

An integral part of DOL's ability to maintain an effective cybersecurity program has been the implementation of corrective actions and improvements based on the findings and recommendations provided by the Office of Inspector General (OIG) through its annual FISMA audit. We continue to value these engagements, have full faith in the integrity of the audit process and in those who execute the audits, and any critical comments in this response are meant to be constructive to help improve the process and value of the results.

In previous years, management has overwhelmingly concurred with the audit team's recommendations (94% concurrence in FY20 and 89% in FY21). However, this year, we have serious disagreement with many of the conclusions reached by the audit team such that DOL management concurred with only 45% of the recommendations and is not able to meaningfully evaluate, report on, and enhance its cybersecurity program based on those portions of the audit report. OMB M-22-05 directs FISMA assessments to evolve to focus on risk-based processes that will provide agencies with sufficient information to consider threat, capability, and impact. Management does not believe this change in approach was adequately adopted for this engagement, as conducted by an audit team from KPMG, as many of the findings focused on minor compliance gaps that do not substantively impact DOL's cybersecurity posture – gaps that are addressed through minimal updates to compliance documentation, many of which had already been accounted for during the audit. Throughout this year's FISMA audit DOL expressed concerns that many of the perceived deficiencies leading to auditors' findings did not present any appreciable risk to DOL, concerns which have not been sufficiently addressed during the audit work or in the report. This has included multiple instances of auditors issuing an evaluation of program maturity which did not appear to consider all the inputs provided by DOL.

While we will provide details regarding each of the audit's findings and recommendations in our later management decision response, we have included examples below as context for our concerns. Importantly, we recognize all the time and effort that went into this year's audit and appreciate the

report's conclusions tied to technical testing in particular - such as the insights provided to enhance DOL's data exfiltration capabilities. However, given the overarching issues described above, and highlighted below, we hope to initiate significant realignment of expectations for next year's FISMA audit, so DOL can focus audit remediation efforts on those areas of greatest impact for DOL's cybersecurity program. As defined by OMB's guidance M-22-05, we hope OIG and KPMG will implement an audit plan in 2023 that focuses on a risk-based approach. The following examples are characteristic of our concerns regarding this year's results:

- **Accuracy:** This report incorrectly interprets DOL policy resulting in unwarranted findings. For example, auditors issued a finding that DOL did not properly authorize a system because the Deputy CIO signed an Authorization to Operate instead of myself, the CIO, who was the system's Authorizing Official. I was on extended leave outside of the country at the time and had assigned the Deputy CIO to act on my behalf, as is customary and documented in the memo "Order of the Chief Information Officer Order of Succession". This finding was based on a statement in the DOL Computer Security Handbook prohibiting the AO responsibility from being delegated; however, in this case, the Deputy CIO was officially acting on behalf of the CIO at the time – the responsibility was never delegated. Furthermore, no substantive deficiency related to the security of the system was identified related to how the system was authorized.

- **Relevance:** The report based certain findings on prior year open recommendations that were not material to this year's review. For example, the report found that OCIO did not adequately monitor supply chain risks because auditors concluded that a prior year recommendation to provide training on conducting reviews of third-party systems remained unimplemented. However, the third-party reviews identified in the prior year finding were not related to DOL's supply chain monitoring. Moreover, the training had actually been performed and evidence of such previously provided.

- **Impact:** The report's core finding around DOL not having yet implemented NIST Special Publication (SP) 800-53 Revision (Rev.) 5 does not identify any significant risk or impact of the DOL's longer timeline for Rev. 5 implementation. For example, the report notes that there were significant changes to privacy controls in Rev. 5 that were not addressed in DOL's privacy program, but summarily reaches this conclusion without actual review of how those privacy controls were being implemented. DOL has many of the associated requirements in place based on controls' previous alignment to NIST SP 800-53 Rev. 4 Appendix J, as well as prior OMB mandates. Significantly, the report identified no actual deficiencies in the protection of personally identifiable information (PII). The same applies for other areas summarily highlighted as deficient because of Rev. 5 not yet being implemented. Regardless of the formal implementation of Rev. 5 itself, DOL has already implemented key Rev. 5 requirements throughout the enterprise, including implementation of new requirements in areas such as vulnerability disclosure, where DHS' Cybersecurity & Infrastructure Security Agency (CISA) has even highlighted the proficiency of DOL's vulnerability management program. But the audit team did not evaluate impact at that level, being more concerned that the number '4' had not been changed to a '5' in documentation.

- **Risk:** Even in some cases where the report did state that a deficiency increased risk, these conclusions were not substantiated and were often wholly inconsistent with the actual risk environment. For example, a key finding in the report was that DOL's Information Security Continuous Monitoring (ISCM) program was deficient because a single security control assessment was not performed properly, and that this deficiency could result in threats and vulnerabilities being overlooked. This finding rested on a determination that a portion of one security control out of 469 applicable security control tests for a single system (out of 13 in-scope

systems) was not included in the system's assessment plan, which ultimately had no bearing on system threats and vulnerabilities.

- **Risk:** Another finding in the report was that a single incident that was untimely reported to US-CERT (reported in 4 hours instead of the required 1 hour) increased risk to the confidentiality, availability, and integrity of DOL information systems and data. This was a single incident out of a sample of only 15 incidents tested by the auditors. DOL reported greater than 99.6% of 547 total incidents to US-CERT within the 1-hour reporting time during FY22. DOL Cyber responses to incident alerts has even been recognized by CISA as an example for other agencies to follow. This single incident was nonetheless rapidly resolved and ultimately presented no increased risk to the single system impacted, let alone to the Department. The report recommends enhanced incident response training to address this finding, which had in fact already been provided, and other measures already taken, prior to the auditors even identifying that issue. This is the very definition of being "Managed and Measurable". Although management presented these facts and examples of the maturity of the incident response program to the audit team, they chose not to consider this information or expand its sample and to focus exclusively on the results of the sample they selected instead of the universe of incidents.

We believe DOL has meaningful opportunities to improve the effectiveness of its cybersecurity program, and management remains committed to remediating cybersecurity risks, including through DOL's planned and on-track transition to NIST SP 800-53 Rev. 5. Unfortunately, this year's FISMA audit results, including the associated OIG FISMA metrics maturity level ratings, will not further this important goal.

Even though not reflected in the audit results, DOL worked diligently over the last year to implement changes to strengthen the maturity of its enterprise-wide cybersecurity program, and progress continues to be made to sustain cybersecurity maturity across all FISMA domains. Some of the significant changes made during FY 2022 include the following:

- Continued to enhance the cybersecurity program, including for areas prioritized under Executive Order (EO) 14028, Improving the Nation's Cybersecurity (May 12, 2021).
- Continued to implement enterprise-wide solutions to enhance encryption, multifactor authentication, IT asset management, incident response and monitoring.
- Continued progress toward the deployment of Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation tools for vulnerability management.
- Continued implementation of new Data Loss Prevention mechanisms.
- Fully transitioned all FISMA systems into Ongoing Authorization.
- Conducted quarterly phishing exercises to promote phishing awareness.
- Continued to advance vulnerability management, which resulted in DOL being recognized by CISA for DOL's outstanding level of engagement on the Vulnerability Disclosure Policy Platform and DOL's commitment to its vulnerability awareness and management process.
- Continued to enhance incident response processes, resulting in DOL's cyber responses to incident alerts being recognized by CISA as a model for other agencies to follow.
- Successfully planned and carried out the FY 2022 DOL Cybersecurity Awareness Month.
- Closed 24 previously open cyber-related OIG findings from previous years.
- Made the following improvements based on OIG recommendations:
  - Developed and implemented a system that maintains and tracks DOL contractors who are required to have PIV cards.
  - Improved physical security processes by updating and improving emergency plan guidance, developed, and distributed active shooter training, and developed a process to automatically notify the Security Center when contractors are separated from DOL.
  - Updated the DOL Risk Management Strategy to appropriately address each activity and task

described in NIST SP 800-39 and NIST SP 800-53.
- Updated the ISCM Plan to include ISCM tiered performance metrics (in accordance with NIST SP 800-137) and a procedure to review and update the ISCM strategy and ISCM Program on a defined frequency, and review and update the policies and procedures for security status monitoring.
- Performed a reconciliation of the current state of each DOL information system and the related classification to the information documented for each system.
- Provided trainings related to removing access for separated DOL employees, patch management process and new guidelines, and user activity review process.
- Reviewed, finalized, and implemented the revised DOL Software Development Lifecycle Manual.

DOL continues to place focus on securing and strengthening its cybersecurity management functions, particularly for areas prioritized under EO 14028. DOL intends to:

- Continue to improve in the adoption of multifactor authentication and encryption of data-at-rest and in-transit;
- Continue the monitoring and protection of critical software and mature capabilities for supply chain risk management;
- Continue efforts to transition DOL's network infrastructure to Internet Protocol Version 6 (IPv6);
- Improve DOL's enterprise log management capability in accordance with OMB M-21-31;
- Continue the implementation of DOL's roadmap for Zero Trust; and,
- Continue Security Operations Center enhancements that will allow DOL to anticipate and mitigate risk, while staying ahead of the evolving threat landscape.

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: Rachana Desai Martin, Assistant Security for Administration and Management
Geoff Kenyon, Deputy Assistant Secretary for Budget and Performance
Paul Blahusch, Chief Information Security Officer
Karl Hellmann, Deputy Chief Information Security Officer
Muhammad Butt, Division Director, Information Security Policy & Planning