Questions for the Record

SUBCOMMITTEE ON GOVERNMENT OPERATIONS
COMMITTEE ON OVERSIGHT AND REFORM
U.S. HOUSE OF REPRESENTATIVES

"FITARA 11.0"

Hearing Date: April 16, 2021

Mr. Gundeep Ahluwalia
Chief Information Officer
Office of the Assistant Secretary for Administration and Management
Department of Labor

Questions from Chairman Gerald E. Connolly, Subcommittee on Government Operations

1. In the 2020 inspector general (IG) report for the top management challenges at the Department of Labor (DOL), the IG noted that there were "ongoing risks to the confidentiality, integrity, and availability of the Department's information." How is your agency planning to secure its data in the near and long term?

Cybersecurity continues to be a top priority at the Department of Labor, and leadership remains committed to continuously strengthening DOL's cybersecurity posture—particularly in the face of new risks associated with the expansion of telework in response to the COVID-19 national emergency, and those exposed by the recent SolarWinds incident.

To address these, and other cybersecurity risks, DOL continues to focus on a number of areas. These include implementing enterprise solutions to enhance IT asset management and automation, and to facilitate near real-time awareness of threats. It also involves deployment of additional Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) tools for vulnerability management, implementation of new Data Loss Prevention mechanisms, and transition of Federal Information Security Management Act (FISMA) systems due for periodic reauthorization into ongoing authorization using a robust continuous monitoring program. In the area of incident detection and response, DOL transitioned its Security Operations Center to provide 24x7 monitoring and response capabilities, to ensure all incident-related activities are captured, reported, investigated, and managed appropriately.

In addition, DOL took a number of steps to improve security in response to the increased teleworking environment. The Department adapted and matured client endpoint security, increased Web Application Firewalling, and implemented cloud-based solutions to enable secure information sharing and manage access in a remote environment. DOL also increased the use of hard tokens for multi-factor authentication to maintain continuity and security for staff unable to obtain and renew Personal Identity Verification (PIV) credentials in person. Finally, DOL provided additional security awareness trainings, including quarterly phishing exercises, to

address increased cybersecurity risks faced by remote users. These measures allowed DOL to seamlessly shift 95% of agency staff to telework, with uninterrupted delivery, while keeping cybersecurity a top priority.

Looking ahead, DOL will continue to focus on strengthening its cybersecurity management functions. The Department intends to: 1) continue to leverage the National Institute of Standards and Technology (NIST) standards and publications to guide its cybersecurity program; 2) mature information security monitoring and protection capabilities across the enterprise to improve cybersecurity efficiency and shorten cyber incident response times, making use of the DHS CDM program wherever appropriate; 3) complete the Department's Security Operations Center (SOC) modernization project as required by Executive Order 13800; 4) secure the Department's IT supply chain as directed in the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act; 5) transition our information security architecture to incorporate a zero-trust approach; and 6) continue to address identified deficiencies to ensure that DOL meets the Cybersecurity CAP Goals in the President's Management Agenda (PMA), and improve the FISMA maturity level. These enhancements will allow the Department to anticipate and mitigate risk, and stay ahead of the evolving threat landscape.

2. Are there any particular changes you would recommend that Congress consider as part of the Federal Information Security Management Act reform efforts and for possible inclusion in a future Federal Information Technology Acquisition Reform Act scorecard?

FISMA has focused leadership attention on cybersecurity, and helped drive DOL's information security improvements. In part due to FISMA, DOL now has, among other things, a 24x7 staffed Security Operations Center, a robust anti-phishing awareness program, and is moving systems to ongoing authorization. Provided the FISMA metrics continue to adjust to stay current with what is important for agency cybersecurity, we see FISMA continuing to be an important tool for cyber improvement.

One possible area for reform would be to change the annual Inspector General assessment requirement to every other year. This would afford agencies (and their OIGs) time to focus on addressing the control weaknesses identified in the biannual assessments. The Committee could also consider evaluating supply chain risk management practices as a component of cybersecurity.

3. What is your agency doing to implement the supply chain risk management practices outlined in the December 2020 Government Accountability Office report (GAO-21-171)?

The security, resiliency, and trust in the information and communications technology (ICT) supply chain is a major area of concern. The recent SolarWinds incidents – while not resulting in any compromise to DOL networks or data – was a clear wake-up call to these risks. DOL is addressing this by A) taking actions on a Departmental level by performing risk analysis on technology proposed for use in the environment and including appropriate cybersecurity

provisions into contracts for IT goods and services; B) engaging with the DHS Cybersecurity and Infrastructure Security Agency (CISA) and the broader Federal community on government-wide approaches to cyber supply-chain risk management as a coordinated Federal approach to supply chain risk management is vital to success; and C) prioritizing the recruitment and hiring of experienced cyber professionals to manage the Department's IT programs and responsibilities.

4. Has DOL fully implemented the 21st Century IDEA Act (Public Law No: 115-336)? What barriers has DOL faced in implementing this law and modernizing its digital services?

In the 2020 report on the IDEA Act, DOL detailed four initiatives demonstrating how it is implementing the IDEA Act and modernizing digital services: two from High Impact Service Providers, the Occupational Safety and Health Administration (OSHA) and the Office of Workers' Compensation Programs (OWCP); and two DOL-wide initiatives.

DOL is pleased to report that it is on schedule with all 4 initiatives, and interim roll-outs are already improving the experience of its public customers. Specifically:

1. OSHA is creating a new portal to administer a program in which management, labor, and OSHA can collaborate on efforts to promote worksite safety and health, by providing a centralized source for applications and self-evaluations. This portal is scheduled to be made available to the public during fiscal year (FY) 2021.

2. OWCP is updating a portal which implements digital claim filing. With this modernization, claimants can access their claim status page, including both medical and pharmacy billing information. This portal is on schedule for full release by the end of calendar year 2021. The only barrier faced was a shortage of programmers who were diverted for COVID response measures.

3. The OneWeb@DOL Initiative ended on September 30, 2020 with 22 DOL agency websites modernized and moved to a web content management system. Completion of the project required migrating more than 225,000 web pages and files to the new web platform.

4. DOL has committed to extensive digitization of forms which are available on public-facing websites, with a focus on web design capabilities as described in Section 508 of the Rehabilitation Act of 1973 as defined by the US Access Board. Every public facing form or page must go through an internal accessibility clearance process, and staff training on Section 508 compliance is offered continually under the auspices of the Branch of Quality Assurance within DOL.

In addition, driven by DOL's Information Technology Modernization Strategy, the Department is aggressively digitizing documents and signatures across the enterprise. The Branch of IT Policy Development & Management is dedicated to the implementation of the Paperwork

Reduction Act of 1995. The resources available for digitization remain a top challenge for the Department.

5. Now that the Software Licensing metric has been retired, what are the next steps the Subcommittee should consider to ensure agencies are effectively using software license inventories to make cost-effective decisions?

The Subcommittee could document and disseminate best practices with regard to software licensing decision making. This would allow agencies to benchmark their practices and processes to ensure they are optimizing their software license purchases.

6. DOL received an "A" on the metric regarding the transition from Networx to Enterprise Infrastructure Solutions. Can you explain what actions DOL has taken that have helped make this transition so successful? How is DOL using this transition to modernize its communications infrastructure?

DOL is leveraging the efficiencies afforded by this new contract to modernize the architecture, capacity, and flexibility of its Wide Area Network (WAN) across the nation. DOL spent time at the beginning of the transition initiative determining how to efficiently compete and award services including how to manage the transition to meet or exceed GSA established deadlines. In advance of the Enterprise Infrastructure Solutions (EIS) transition, DOL successfully migrated approximately 300 office locations to the Department's enterprise Unified Communications platform. The new network-based phone service enabled DOL to converge its data and voice capabilities, resulting in a significant reduction in the amount of telecommunication services needing to be transitioned and allowing for an acceleration of the transition schedule. The Unified Communications platform is less expensive to maintain and more flexible in response to evolving office staffing patterns, and was therefore critical in enabling the Department to seamlessly transition to a maximum telework posture during the pandemic. The new EIS contracts will help DOL to continue to implement Unified Communications at sites still requiring modernization as well as improve cost control and mission productivity through improved network connectivity and scalability based on need. As a result, DOL is prepared for the network demands of the future, especially in the post-pandemic world where site demand will change.

7. How has DOL used the General Services Administration Application Rationalization Playbook when developing strategies to modernize high value assets or core mission applications?

While GSA's Application Rationalization Playbook is a good resource for modernization recommendations and best practices, it was not specifically leveraged as part of DOL's modernization efforts. However, the process in use at DOL aligns with the Playbook. DOL

inventoried its systems and applied a specific set of criteria with the express purpose of developing a prioritized list of candidate systems for modernization. As funding becomes available, the Department has used this prioritized list as one of its decision points for moving forward with a modernization effort.

8. What is the status of adoption and implementation of the Technology Business Management framework at DOL? What challenges, if any, has DOL faced throughout this implementation?

DOL has implemented Technology Business Management (TBM) as required for external reporting. When TBM was first introduced, IT services were provided under a federated model where, for the most part, each subagency was responsible for its own IT services. Under this model, it was difficult to utilize the TBM framework as the basis for decisions. Each agency applied their own interpretation of the IT Tower and IT Cost Pool definitions so there was no consistency across the Department. DOL has since moved to a shared services model where the Office of the Chief Information Officer (OCIO) provides both the infrastructure and the mission application IT support services for subagencies. Under this model, OCIO is able to apply the same interpretation of the IT Tower and IT Cost Pool definitions across the enterprise and increase the accuracy of its external reporting. This increases the ease with which the TBM framework can then be utilized as the basis for decisions. However, full implementation of the TBM framework requires extensive cost and usage data which currently resides in multiple systems.