FY 17 IT Modernization & Integration Overview

DOL's IT Modernization Program seeks to consolidate nine aging infrastructures while improving the level and quality of IT services to improve mission performance. IT modernization means employees are able to better perform their jobs and DOL agencies can more effectively provide services to citizens. The multi-year modernization initiative is improving cross-agency collaboration, eliminating cost redundant infrastructures, achieving federal goals for energy efficiency, and creating a more reliable, secure and consistent IT infrastructure. To lead the modernization initiative, OCIO is transforming from a small IT center supporting 3,000 employees to an enterprise IT organization supporting 23,000 Federal staff and contractors. The last five years provide evidence of progress as well as challenges to the success of IT modernization.

IT Modernization Progress Indicators

Since 2011, OCIO IT improvements have produced cost savings through efficiencies and cost avoidance, higher staff productivity, and increased capacity to implement mission. During this time DOL formalized the role of Chief Information Officer, responded to OMB and FITARA requirements, and implemented several notable IT projects summarized below. OCIO has proven that it can deliver modern IT services, on time and within budget, even with limited resources.

Infrastructure Integration: A critical modernization objective has been to consolidate nine separate and disparate DOL Agency IT infrastructures into one unified infrastructure. To date, DOL has performed a "lift and shift" integration of data centers for 25 of 27 agencies. In 2013, DOL launched the data center consolidation initiative (DCCI) in Silver Spring, MD, acquiring an uninterruptible power source that reduces the risk of outage, and enabling DOL to close over 40 data centers and stand up the Failover/Disaster Recovery site in St. Louis, MO. The initiative increased network, storage, computing and backup operational capabilities, and complied with an OMB mandate. However, the technical integration of the network and most of the infrastructure integration has not occurred, and is funding dependent; these are critical outcomes for the full deployment of Unified Communications (below). The two outstanding infrastructures: Office of the Inspector General (OIG) and Bureau of Labor Statistics, were recognized as special cases due to security concerns, and alternative options are being considered to maximize security, transparency, and efficiency.

Unified Communications (UC) - Wireless, Mobile, VTC, VoIP: OCIO developed a blueprint to modernize DOL's infrastructure and securely provide and implement wireless, mobile device management, and unified communication including VoIP (voice over IP) and VTC (video teleconferencing). This is demonstrated through the first initiative of the UC project to replace the decades old DOL network infrastructure. By the end of February 2017, UC will have implemented wireless access throughout the Frances Perkins Building (FPB) representing 25% of DOL staff, to be followed by wireless deployment to regional staff in subsequent fiscal years, dependent on funding. In the first quarter of FY 17, upgraded video-teleconferencing (VTC) will be deployed in four FPB conference rooms, and 500 FPB staff will receive Voice over Internet Protocol (VoIP) phones and training in the first wave of deployment. To advance the UC initiative Department-wide, DOL will need to fund technical infrastructure integration, and

provision wireless, VTC and VoIP for all locations. An additional UC benefit for select DOL agencies will be the upgrade of call centers across the country.

Cloud Email: DOL was one of the first federal agencies to successfully migrate to the Microsoft 365 federal community cloud; an OMB target for all agencies by 2017. DOL staff migrated to Cloud Email in FY 2014 (100% of DOL staff except BLS). Prior to Cloud Email the greatest staff pain point was lack of email storage. Cloud email added practically infinite storage capacity and modern cloud capabilities for the maintenance cost of one system versus the former nine separate legacy systems. In addition, Cloud Services provide DOL options for the deployment of mobile devices across the Department.

CyberSecurity: In 2015, DOL accelerated the timeline for implementing two-factor authentication (PIV Card Logon) to secure the identity and system access for over 98% of its general users and 99% of its privileged users. Leveraging DHS' Continuous Diagnostic and Mitigation (CDM) Program, DOL avoided approximately S3.5 million in expenditures for security monitoring tools. Through the implementation of CDM tools, DOL decreased its security vulnerabilities by approximate 95%, from 1 million high security vulnerabilities to below 10,000 in just 18 months. DOL will continue to utilize the DHS CDM Program for additional security tools and safeguards, and related cost avoidance.

DOL IT Challenges and Solutions

DOL has made progress toward the IT modernization goal, however the original mission of technical integration of the infrastructure and applications lies ahead. In addition, several challenges require a reset of Agency relationships and OCIO processes supporting enterprise IT success.

Lack of trust between OCIO and Large Agencies: Now in the sixth year of IT consolidation, the performance, benefits and costs of integration efforts have been questioned by a number of Agencies. Concerns that have been raised include: lack of transparency, infrastructure and service performance, costs, and consolidation objectives.

- **Infrastructure and/or service performance are perceived to have decreased** since consolidation. Common examples provided include network failures, Enterprise Service Desk (ESD) service shortfalls, website and application shutdowns, and grievances regarding IT processes. Moving forward, OCIO and the Agencies are working to better benchmark performance, validate pain points, and demonstrate service performance.
- **IT service costs post-consolidation are perceived to have increased** and are considered unpredictable. Over the past year, OCIO has worked to provide financial transparency through the yearly IT Service Orders, monthly Agency IT Service and Funding Reports, and in-person meetings to explain costs and answer questions. OCIO is committing to providing additional financial transparency in FY '17.
- **Consolidation objectives have not yet been achieved**. While both OCIO and Agencies understand the potential benefits of IT consolidation and modernization, many of the anticipated benefits are dependent on technical integration, which has not occurred yet. A

challenge for the next Secretary will be developing and implementing an integration plan given limited budgetary resources.

In August 2016, DOL leadership sought to create new mechanisms for OCIO and DOL agencies to work more collaboratively. OSEC established a Steering Committee which then identified an integrated project team (IPT) process for OCIO and DOL agencies to begin to work together in a more concerted manner. The IPT Steering Committee includes nine career participants from across DOL agencies, and is led by the Secretary's Chief of Staff. The IPT Steering Committee launched with the goal of coordinating change in the best interest of the Department.

Insufficient strategy development and implementation: Technical and organizational transformation initiatives necessary to modernize infrastructure, reduce technical deficit, and consolidate infrastructure are not fully underway. DOL has completed some integration planning to include an Information Resources Management Strategic Plan and Enterprise Roadmap as directed by OMB. OCIO has also developed a future state Technical Architecture Strategic Roadmap (TASR). However, there is no plan to modernize and consolidate Agency legacy applications. A Department-wide strategic IT plan with buy-in from all parts of the organization needs to be developed.

Weak IT Governance and Oversight Structures, and limited FITARA implementation:
DOL established a minimally effective IT governance model in 2011 to enable IT services, investments, and solutions to comply with federal mandates. IT governance groups include the Enterprise Implementation Committee (EIC), IT Acquisition Review Board (ITARB), Program Review Board (PRB), Strategic Business Alignment Committee (SBAC), IT Service Management (ITSM), and the Field IT Forum (FIF). The perception is that the IT governance committees are weak and do not work. As a result, an IPT has been established to consider how to strengthen DOL IT governance and Agency engagement in governance. With regard to FITARA, DOL has made minimal progress moving forward with its OMB approved plan. Implementing a streamlined, cohesive and well socialized governance process will be key to achieving FITARA, OMB and DOL integration and service targets for modernization.

IT Funding: Publicly available funding data shows that DOL IT spending is predominantly on Operations and Maintenance (O&M) activities. OCIO makes difficult choices between addressing IT risks, meeting immediate needs, governance, and planning long-term IT modernization efforts. "Lift and shift" integration has not resulted in savings for DOL. The CIO.gov dashboard compares levels of IT spending by Agency and identifies benchmarks for new technology and O&M expenses. DOL spends less, at 14.1%, for new and innovative technologies (referenced as provisioned development, modernization and enhancement services) than the government-wide median of 22.9%, contributing to DOL's technical deficit accrued over decades. Understanding this technical deficit and planning a path out of it is dependent on allocating resources to DOL's IT Modernization initiative in the coming years.

Forward Focused DOL IT Agenda FY 2017-2018

Moving forward in FY 2017, OCIO drafted guiding principles for prioritizing IT initiatives required by DOL, planned for the enterprise and requested by an Agency. OCIO will focus on the implementation of funded Departmental priorities and IT projects, address federally mandated OMB and FITARA requirements to the extent possible, and mitigate weaknesses affecting the success of IT Modernization.

FY17 Guiding Principles for Prioritizing IT Initiatives

- **Improve Mission/Customer Focus**: Identify opportunities to improve critical IT capabilities that will result in constructive and collaborative outcomes for DOL and Agency missions, and improve customer relationships. Implementation of MS Windows 10/Office 2016, ESD Self Service Portal, and Unified Communications would enable DOL to fulfill mission areas despite flat/reduced resources.
- **Modernize IT Infrastructure/Improve Service Levels**: Lead IT infrastructure modernization activities, and align budget to projects that improve infrastructure and service levels. This includes continuous improvement of foundational IT services such as IT network, email, hosting, ESD, desktop services, onboarding, office moves, etc., as well as the implementation of Target Architecture Strategic Roadmap (TASR) and technical integration plans.
- **Bolster Information Security**: Implement DHS' Continuous Diagnostics and Mitigation (CDM) Program, Identity and Access Management initiative, and track vulnerabilities that threaten system and mission security. Continue investments in ATO re-certifications, RSA Token support, and enterprise security defenses.
- **Improve Operating Efficiencies**: Identify key processes and metrics that will elevate performance, support FITARA implementation, and assist OCIO in focusing operational efficiencies through initiatives such as the 2017 hardware refresh, IT change and configuration management, and energy monitoring.