

Information Resources Management (IRM) STRATEGIC PLAN

Fiscal Years 2014-2018



UNITED STATES DEPARTMENT OF LABOR

Message from the Chief Information Officer



In 2010, the Department of Labor (DOL) Office of the Chief Information Officer initiated an Information Technology (IT) Modernization program. The program goal is to use “information technology strategically to modernize the Department’s infrastructure and support project-oriented initiatives that demonstrably improve IT program performance and contribute to achieving the Secretary’s outcome goals.”

As the Chief Information Officer, I continue to work towards this goal. To that end, I am pleased to present the Department of Labor’s Information Resources Management Strategic Plan (IRM SP). The IRM SP defines an informed strategy to integrate disparate efforts across the Department to achieve greater effectiveness. It also communicates a strategy to consolidate resources and services for greater efficiency.

While the road to greater efficiency does not come without its challenges, I believe that with these challenges come the greatest opportunities. The goals and objectives in this plan outline the overall IT strategy DOL will follow in Fiscal Years 2014 – 2018, including but not limited to consolidating disparate IT infrastructures; enabling wireless capabilities not only for national but also for the regional and remote workforce; enhancing network security; promoting information sharing and accessibility; delivering smarter IT; and increasing the quality of customer service.

To keep on target in meeting these goals, over the course of the next several fiscal years DOL will be transforming its IT organization. Using fundamental principles and best practices in leadership and management, the Department must identify, assess, and navigate organization specific challenges. For DOL, there are several considerations that inform the IRM SP:

- The Department level organization and cultural environment is critical to the success of agency mission and information technology factors. It is reasonable and prudent to assess and consider the rate at which the organization can adapt to change.
- DOL agencies’ missions are complementary, but differ in application and data requirements, which varies the degree of external data sharing and integration that is required and allowed as well as the degree of organizational support for those agencies.
- The majority of DOL’s workforce is located, and interacts with the public, in regional offices and distributed locations throughout the U.S. Therefore, infrastructure services (i.e., telecommunications) must be available and consistent across locations.
- DOL has long operated under a federated IT model which optimized services from an individual agency perspective. However, we will shift to a model which optimizes enterprise-wide IT services while ensuring that end-user services are improved or at least maintained at the same level.

In spite of the inherent challenges and complexities within IT, I am committed to achieving our IT vision and to building a future-ready organization delivering better, faster, and more robust services to American citizens and businesses.

Executive Summary

IT modernization continues to be a top priority for DOL senior leadership. In the fall of 2014, Deputy Secretary Chris Lu said, “I see information technology as the game changer to give our field staff the best technology capabilities possible to enhance their mission performance.” The Deputy Secretary acknowledged in order to be a future-ready organization, DOL must first build a solid foundation to include a consolidated, integrated, updated, and secure IT infrastructure.

With senior leadership’s commitment to IT modernization, DOL is poised to be a future-ready organization guided by this plan which provides the strategic IT direction for the Department’s use of information resources to support agency missions and guides IT planning and decision making activities. Execution of this plan, by all agencies, will enable the organization to deliver better, faster, and smarter services to citizens and businesses. The IRM SP includes five strategic goals to be accomplished over the upcoming years:

- 1) Modernize the IT Infrastructure
- 2) Share Information
- 3) Deliver Smarter IT
- 4) Enable the Workforce
- 5) Enhance IT Management

Modernizing the IT infrastructure supports the priority of building a future-ready government, one that is both efficient and effective. This will be accomplished by consolidating, integrating, and updating the IT infrastructure; building out a wireless and unified communications infrastructure; and securing the IT infrastructure.

Sharing information enables an open and accountable government by making information available to the public. This will be accomplished by promoting information sharing and data accessibility; preserving electronic records; providing quality customer service experiences; securing information exchange; and improving electronic and information technology accessibility.

Delivering smarter IT enables the Department to be more efficient. This will be accomplished by enhancing digital services; leveraging IT shared services and establishing a central management capability; pursuing smarter IT delivery through better, faster, and more robust services; and improving strategic sourcing opportunities.

Enabling the workforce supports the priority of having a future-ready workforce. This will be accomplished by promoting a flexible working environment; improving learning and training opportunities; encouraging innovation; and promoting cybersecurity awareness.

Enhancing IT management enables the Department to be more effective in utilizing IT to deliver agency business missions. This will be accomplished by improving IT project management; strengthening cybersecurity management; and having proactive disaster recovery planning.

TABLE OF CONTENTS

Message from the Chief Information Officer i

Executive Summary ii

1 Introduction..... 1

 1.1 Purpose..... 1

 1.2 Key Assumptions and Constraints 2

 1.3 Scope and Audience..... 2

 1.4 Roles and Responsibilities 2

 1.5 Department Vision and Mission 3

2 IT Strategic Direction 4

 2.1 Goal 1 - Modernize the IT Infrastructure..... 5

 2.2 Goal 2 - Share Information 7

 2.3 Goal 3 - Deliver Smarter IT 11

 2.4 Goal 4 - Enable the Workforce 14

 2.5 Goal 5 - Enhance IT Management 17

3 Strategic Framework 19

 3.1 DOL’s Integrated IT Governance Approach 20

APPENDIX A – OMB Requirements Matrix 25

APPENDIX B – Strategic Goal Traceability 27

APPENDIX C – IRM SP Update Process..... 29

APPENDIX D – Departmental Drivers 30

APPENDIX E – Governmental Drivers..... 31

APPENDIX F – IT Governance Structure 32

APPENDIX G – List of Acronyms 35

LIST OF FIGURES

Figure 1: DOL IT Strategic Planning Line of Sight 1

Figure 2: DOL IT Strategic Direction..... 4

Figure 3: DOL IT Governance Structure 20

Figure 4: DOL IT Investment Management Framework 21

Figure 5: IRM SP Update Process 29

LIST OF TABLES

Table 1: DOL IT Governance Bodies 33

1 Introduction

For more than a century, the Department of Labor (DOL) has been helping Americans find employment, feel more secure in the workplace, and benefit fairly from their hard work. The role of Information Technology (IT) in helping to deliver DOL’s core services has grown ever more important over the past several decades, and today IT is an indispensable contributor to the success of the organization. With a modern, unified IT infrastructure and the application of modern technology capabilities, the Department will be better positioned to more fully achieve its mission.

The Department’s policies, programs, and initiatives will expand access to opportunities for America’s workers and their employers, a cornerstone of the Secretary’s vision and a critical role in the Administration’s effort to build an economy of opportunity. IT priorities in support of this vision will periodically be revised to consider evolving technologies and cost models so that resources can be reallocated to maximize return on investment. As a result, this Information Resources Management Strategic Plan (IRM SP) is a working, living document updated periodically to maximize the positive impact of information resources in fully realizing the Department’s mission of serving American citizens and businesses.

1.1 Purpose

[OMB Requirements: AXXA, AXXB]¹ This plan provides the strategic IT direction for the Department’s use of information resources to support agency missions and guides IT planning and decision making activities. It is a forward-looking strategy directly supporting the Secretary’s vision described in the DOL Strategic Plan. A strategic planning traceability matrix is located in **Appendix B** showing how DOL’s strategic objectives are supported by this plan and how it advances these objectives. **Figure 1** below illustrates the Department’s IT strategic planning line of sight with a document hierarchy.



Figure 1: DOL IT Strategic Planning Line of Sight

¹ Throughout this plan, brackets [] appear in applicable paragraphs for the Office of Management and Budget’s (OMB) *FY 2013 PortfolioStat Guidance* (M-13-09) requirements. **Appendix A** includes a listing of these OMB requirements with corresponding location(s) in this document.

1.2 Key Assumptions and Constraints

IT planning decisions at DOL are influenced by its vision and goals, as well as economic, cultural, and technological assumptions and constraints. Among these are:

- IT resources will be focused on activities and initiatives to support the Department’s and Administration’s priorities.
- IT Modernization and technology can significantly improve the effectiveness and productivity of mission operations, and enable delivery of new public services.
- New technology allowing faster and easier access to more timely and evolved data will trigger demands for new IT services.
- Funds available will be less than the demand for them.
- IT personnel skills, knowledge, and abilities will change as the Department transitions to more complex IT technology models.
- IT initiatives must consider the ability of the Department to absorb cost, risk, and technological change while maintaining continuing operations.

These assumptions and constraints impose conflicting demands on the Department’s IT program. While increased demand for more and better IT services grows, the pressure to limit budget growth will continue. The strategy to modernize, expand and improve IT services to support agency mission is dependent on adequate funding and highly capable and empowered IT staff.

1.3 Scope and Audience

This plan was developed leveraging both Departmental (internal) data inputs and Governmental (external) data inputs as drivers and articulates the Department’s IT strategic direction for fiscal years (FY) 2014 – 2018. The target audience for the plan is the entire Department including all agencies, bureaus, offices, and programs (“agencies”).

1.4 Roles and Responsibilities

[OMB Requirement: DXXA] The Chief Information Officer (CIO) position was established by the *Clinger Cohen Act* (CCA) to “ensure agency compliance” with the *Paperwork Reduction Act*, and to “carry out” the agency’s responsibilities in seven discrete areas: (1) information resources management; (2) the collection of information and the control of paperwork; (3) information dissemination; (4) statistical policy and coordination; (5) records management; (6) privacy and security; and (7) IT technology. Congress later built on and clarified CIOs’ responsibilities through the *E-Government Act* (which tasked CIOs with overseeing the development of a fully-modernized federal workforce, among other things), the *Federal Information Security Management Act* (FISMA) (which directed CIOs to develop and maintain an agency-wide information security program among other things) and the *Federal Information Technology Acquisition Reform Act* (FITARA) (which gave CIOs a more “significant role” in all agency “decision processes” concerning IT). As is clear from these authorities, Congress envisioned the CIO as an executive level leader who would be a member of the Department’s top level management team and play a critical leadership role—driving policy developments and ushering in necessary reforms to help control system development efforts, better manage technology spending, translate business needs into IT investments, and achieve real, measurable improvements in mission performance.

OMB has implemented Congress's mandate through various directives and policy statements. For example, *OMB Circular A-130* outlines the specific processes a Department must implement to fulfill the requirements of the CCA and subsequent related statutes, and includes the establishment of an Department-wide Enterprise Architecture to define the future state of an Department's IT environment such that it closely aligns technology with the Department's mission. OMB's *Memorandum on Chief Information Officer Authorities* (M-11-29) states that in "addition to fulfilling their statutory responsibilities," CIOs have the authority and lead performance role in the following four areas: Governance, Commodity IT, Program Management, and Information Security. With responsibility in these four areas, the CIO is held accountable for lowering operational costs, terminating and turning around troubled IT projects, and delivering meaningful functionality at a faster rate while enhancing the security of information systems. These authorities also enable the CIO to reduce the number of duplicative systems, simplify services for American citizens, and deliver more effective IT to support DOL's mission.

Within DOL, the Office of the Chief Information Officer (OCIO) is responsible for updating and maintaining the IRM SP.

1.5 Department Vision and Mission

The Department's vision and mission below set the strategic direction and way forward, and are supported by the Department goals and objectives.

Vision: *Promoting and protect opportunity*

Mission: *Foster, promote, and develop the welfare of the wage earners, job seekers, and retirees of the United States; improve working conditions; advanced opportunities for profitable employment; and assure work-related benefits and rights*

The IT vision, strategic goals, and objectives reflected in this document are in alignment with this vision. Achieving the Department's vision and mission requires the efforts of over 16,000 federal employees and several thousand more contracted resources, working in numerous specialized organizations.

2 IT Strategic Direction

As part of the strategic planning process, the Department defined a vision of its future IT environment to support and enable it to successfully achieve its mission goals. This vision encompasses a modern and unified IT environment incorporating the Administration’s priorities encompassing digital services, open data, and world-class customer service. **Figure 2** below illustrates the Department’s IT strategic direction including the overarching vision, five strategic goals to achieve the vision, and the objectives supporting each strategic goal.

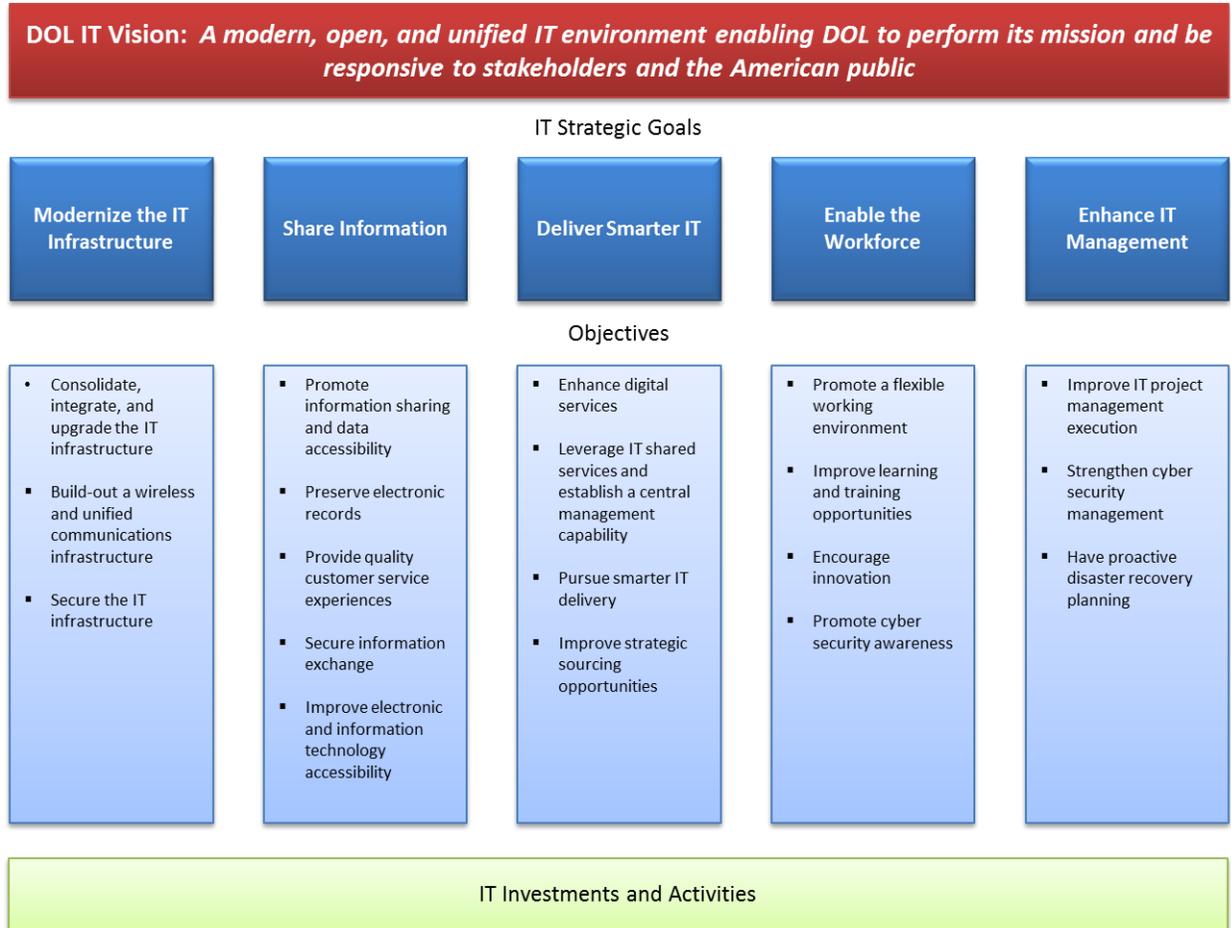


Figure 2: DOL IT Strategic Direction

Each of these goals is described in further detail in the subsections below. In addition, each goal is supported by a set of objectives describing a specific business need, activities the Department is performing, or plans to perform, and how it will realize the goal. Departmental and agency IT investments and activities are planned then executed in order to accomplish these objectives, which in turn supports or directly contributes to achieving an IT strategic goal.

2.1 Goal 1 - Modernize the IT Infrastructure

Modernization of the IT infrastructure supports the Administration's priority and commitment to building a future-ready government. A modern IT infrastructure will deliver better, faster and more robust services; increase quality and value in the Department's core functions; and enhance business mission program productivity. The centerpiece of the IT modernization effort is the consolidation and integration of disparate agency IT infrastructures with the goals of streamlining as well as improving IT operations and customer service. The resulting IT service organization will provide a standardized technical infrastructure that reduces costs by eliminating duplicate infrastructure components, maintenance, and operating expenses.

Other IT infrastructure modernization activities include the consolidation of data centers (adherent to the Federal Data Center Consolidation Initiative) as well as upgrades to and standardization of the technology infrastructure. These activities will strengthen the Department's cybersecurity posture and will provide a foundation for the Digital Government Integrated Platform (DGIP) initiative. The technology infrastructure upgrades are anticipated to enable voice over internet protocol (VoIP), wireless capabilities in DOL Headquarters as well as regional and remote sites, and video teleconferencing (VTC) services—collectively known as unified communications.

Overall, the consolidation and integration of disparate agency IT infrastructure operations will allow the agencies to focus on their business mission IT and associated performance instead of having the burden and challenges of managing day-to-day IT infrastructure operations. To that end, modernizing the IT infrastructure will be accomplished by focusing resources on, implementing, and then delivering results for the following objectives:

Objective 1.1: Consolidate, integrate, and upgrade the IT infrastructure

[OMB Requirements: HXXA, HXXB] The Department is committed to delivering better, faster, and more robust services to its workforce and to American citizens and businesses it serves. In order to accomplish this, the consolidation and integration of disparate agency IT infrastructures needs to be completed. The Employment and Training Administration (ETA) and Mine Safety and Health Administration (MSHA) IT organizations were integrated in FY 2014 leaving four remaining agency IT infrastructures—the Office of Administrative Law Judges (OALJ), the Employee Benefits Security Administration (EBSA), the Office of the Inspector General (OIG), and the Bureau of Labor Statistics (BLS) - to be integrated in future fiscal years.

Additionally, IT infrastructure upgrades, including Department-wide switch and server upgrades, will increase bandwidth enabling DOL's office locations, including national, regional, and remote to have faster connectivity to enterprise and mission IT systems and solutions. These IT infrastructure upgrades, in addition to the transition to Internet Protocol Version 6 (IPv6), prepare a foundation for unified communications and, in future years, a Virtual Desktop Infrastructure.

Furthermore, the consolidation of data centers helps lower IT operational and associated maintenance costs; reduces the consumption of energy; reduces the real estate footprint;

strengthens the IT security posture; and encourages the migration of IT systems toward more efficient computing platforms and technologies like cloud computing. The consolidation and optimization of data centers is driven by the Department's Data Center Consolidation Initiative where agencies are strongly encouraged to migrate their critical server production activities from mixed use buildings to the Department's state-of-the-art, off-premise tier one data center facility. The Department plans to reinvest any savings from the consolidation of data centers into the unified IT infrastructure and/or into new enterprise-wide technologies such as unified communications.

Objective 1.2: Build-out wireless and unified communication infrastructures

In order for the Department to deliver better, faster, and more robust services to American citizens and businesses it serves, the workforce requires the capabilities to work from anywhere at any time. This objective encompasses the build-out of wireless and unified communication infrastructures to support modern, seamless communications and wireless access. Both infrastructures will enable greater workforce collaboration and connectivity through unified communications, VTC, and wireless services such as mobile device management (MDM) and mobile content delivery (MCD). The Department plans to pilot unified communication and VTC infrastructures in the Washington, DC area office locations then expand to regional and remote locations where available.

Objective 1.3: Secure the IT infrastructure

As adversaries continue to increase the sophistication, frequency, and boldness of attacks on federal IT systems and websites, the Department is responding by aggressively upgrading its cross-enterprise defensive capabilities. This objective focuses on defending the shared IT environment by heightening visibility into agency security operations. DOL will achieve this through the enhanced collection, normalization, and synthesis of data to allow for optimized reporting. Optimized reporting in turn provides senior management with true situational cybersecurity awareness in support of effective decision-making. Furthermore, the confidentiality, integrity and availability of IT systems must be maintained. By ensuring the IT environment is secure, the Department significantly mitigates the risk of compromise to the public's personal information, degradation of safety-related systems, and impacts to the economic health of our country from unauthorized access to highly sensitive economic data.

Another way DOL actively secures the infrastructure is through compliance with OMB's *Trusted Internet Connection Initiative* (M-09-32) which mandates the reduction of external network access points. The Department is implementing this through the integration and consolidation of disparate agency Local Area Network and Wide Area Network infrastructures into a single enterprise infrastructure and will continue to secure the IT infrastructure by enhancing operations of the computer incident response capability. One major enhancement includes collaborating with the Department of Homeland Security (DHS) and using tools from the DHS Continuous Diagnostics and Mitigation program. These tools allow strengthened continuous monitoring of software assets, database activity, vulnerability management, and website security.

In addition to the DHS program, DOL's Security Operations Center (SOC) uses continuous monitoring tools to scan workstations, servers, network, and security perimeter devices for any indications of potential risk. These monitoring tools allow the SOC to identify all devices on the infrastructure, monitor all traffic across the infrastructure, maintain compliance with Departmental and federal security standards (for workstations, servers, network devices, web servers and databases attached to the infrastructure), and identify threats and exploitation attempts.

2.2 Goal 2 - Share Information

The Administration has prioritized the need for a transparent, collaborative, and participatory government with the President's *Transparency and Open Government memorandum*² and OMB's *Open Government Directive* (M-10-06). An open government promotes accountability by sharing and making information available to the public regarding government activities. This encourages partnerships and cooperation within the federal government, as well as with public and private institutions. In addition, OMB's *Open Data Policy* (M-13-13) instructs agencies to manage information as an asset throughout its life cycle, promote openness and interoperability, and properly safeguard systems and information. The ability to securely share information is foundational for the organization to operate in an open manner, especially with a diverse and widely distributed workforce. In response to this Directive and Policy, the Department has a comprehensive [Open Government Plan](#) and has undertaken several efforts to make DOL more transparent, accountable, and responsive to American citizens and businesses.

Sharing and managing information as an asset will be accomplished by focusing resources on, implementing, and then delivering results for the following objectives:

Objective 2.1: Promote information sharing and data accessibility

[OMB Requirement: GXXA] Information sharing and data accessibility requires the organization to make data and information open, available, and accessible for use by others within the Department, across the federal government, and to the public. DOL understands the value of open and accessible data and how it can fuel innovation within the federal government or private sector. The Department is committed to information openness, information system interoperability, and managing information as an asset throughout its life cycle - as described in the *Open Data Policy*.

An example of how DOL provides open and accessible data is the Department's [Enforcement Data](#) website. This site provides searchable access to DOL enforcement data collected by EBSA, MSHA, the Occupational Safety and Health Administration (OSHA), the Office of Federal Contract Compliance Programs (OFCCP), and the Wage and Hour Division (WHD). In addition to the added value of access to aggregate enforcement data, this site also provides public access to a variety of previously unpublished enforcement information. As a result of its success, it has been used by press organizations and outside stakeholders to look at industry and corporate trends and has spurred thinking on how DOL can use its data more effectively to convey the mission and value of the Department's work.

² President Barack Obama, Memorandum on Transparency and Open Government, Jan 2009.

Another example is the Department's [Grant Application and Award Database](#) which provides a central online location for the public to learn about DOL's competitive grant programs. Not only can users access an assortment of financial and programmatic information on funded grants, the website also links prospective applicants to tools and resources needed to craft a competitive grant application. Perhaps most importantly, the site allows the public to search, view, and download abstracts of all grant applications for the Department's discretionary grant programs as well as the full technical proposals from grant applications selected for award.

Furthermore, DOL provides the public data listing which includes datasets made available through a single external application programming interface (API) to the public by the Department's public website, [DOL.gov](#). These datasets can be utilized by software developers to create or enhance smart phone applications and/or web-based applications. This external API portal acts as a smart communications hub to control and manage application data requests from one or more interconnected datasets, which improves the efficiency and effectiveness of data queries as well as the overall potential of supporting more advanced applications. The external API utilizes open standards served by an Open Data Protocol (OData) implementation. OData allows data access from web service consuming applications and supports many data source technologies. In addition to making data accessible via the external API, the Department also publishes datasets to [Data.gov](#), the federal government's data repository. Also, building on the success of the external API, a single *internal* API is planned to be developed to promote and enhance cross-agency data sharing. The internal API will provide a highly efficient, low cost approach for promoting interoperability between agency data and information systems.

There are two other ways in which the Department will promote information sharing and data accessibility. The first is the implementation of *Executive Order 13673 Fair Pay and Safe Workplaces* in which DOL has the primary role as system owner to share information (i.e., labor law violations) with the General Services Administration (GSA) as well as making this information accessible online to the public in 2016. The second is the implementation of the *Digital Accountability and Transparency Act of 2014* (DATA ACT) and OMB's *Guidance on Increasing Transparency of Federal Spending by Making Federal Spending Data Accessible, Searchable, and Reliable* (M-15-12) in which DOL will provide data to Treasury through the [USASpending.gov](#) website under the "data-centric" approach using a standard data exchange ("DATA Act Schema"). The DATA Act Schema, published on GitHub, is designed to give DOL a baseline for building useable databases to aggregate, collate, and summarize its financial data around contracting, loans and grants.

Lastly, the DGIP initiative will also promote and support information sharing and data accessibility with a strategic data management (SDM) capability to include data/digital asset management and data modeling, repository, and analytics. This SDM capability will allow agencies to collect, manage, and share data inclusive of audio, video, and photographic images across agencies using a standard data reference model, a data repository, and a data analytics service.

Objective 2.2: Preserve electronic records

In response to OMB's *Directive on Managing Government Records* (M-12-18) and *Guidance on Managing Government Records* (M-14-16) the Department will work towards developing an enterprise records management solution to manage all email and permanent electronic records in an accessible, electronic format. To that end, the Department is exploring the use of National Archives and Records Administration's (NARA) Capstone Approach as a solution to temporary and permanent email records management in efforts to meet the December 31, 2016 deadline as directed in M-12-18. NARA's approach coupled with the retention and archiving capabilities provided by DOL's cloud-based email solution may be a feasible means to establish a solution to manage email in the cloud.

The anticipated cloud-based solution will support both records management and litigation requirements providing the necessary capabilities to identify, retrieve, and retain email records for as long as they are needed. In addition, DOL will undertake a planned, collaborative effort between the OCIO, Business Operations Center, and the agencies to establish policies and procedures to manage *permanent* records electronically by December 31, 2019.

Objective 2.3: Provide quality customer service experiences

Providing quality customer service experiences are crucial for the Department to accomplish its mission – the public must be able to contact and have easy access to agencies through multiple channels. Responses must be timely, accurate, complete, and consistent with responses originating from subject matter experts and answers relayed to the customer in a timely, professional, and courteous manner.

In support of and in response to *Executive Order 13571* and OMB's *Guidance on Streamlining Service Delivery & Improving Customer Service* (M-11-24), the Customer Service Program Office (CSPO) was established to ensure all customer requests are handled in an efficient and effective manner regardless of the communication channel used to initiate contact. The CSPO leads, coordinates, and monitors customer service initiatives cutting across all organizational lines of the Department. To assist with customer service automation, a cloud-based Customer Relationship Management (CRM) shared service initiative was piloted in FY 2014 and may be expanded to other agencies in the upcoming years. The CRM pilot contains a robust knowledgebase enabling information to be found and delivered both quickly and accurately. It also provides a self-service option, allowing customers to find answers to their questions and receive updates on case status.

The CSPO also provides agencies with guidance and assistance on a wide range of customer service-related activities, including the establishment of customer service standards, customer feedback collection, adoption of customer service best practices, and implementation of tools to enhance the customer experience. [OMB Requirements: BXXA, BXXB, BXXC] Agencies analyze and measure customer satisfaction and evaluate their customer-facing services. In addition, they are in control of improving usability, the availability, and accessibility of their services, including the optimization of services for mobile use as well as evaluating their customer-facing services to advance agency performance goals.

Objective 2.4: Secure information exchange

[OMB Requirement: GXXB] All federal agencies need to protect their information assets with the use of strong authentication, as required by *Homeland Security Presidential Directive 12* (HSPD-12). Information-in-transit must also be secured and must only be passed through an approved Trusted Internet Connection (TIC). Implementing strong authentication will reduce the risk associated with unauthorized access to information systems. Adding a second factor of authentication dramatically reduces the potential of attack through password cracking and phishing, thereby fortifying the Department's IT security posture. Similarly, by fully utilizing TIC, the Department has reduced the risk of having information-in-transit intercepted and/or compromised.

Progress is being made toward strong two-factor authentication by using a token-based authentication technology as the primary tool for allowing administrators to monitor DOL's networks and information systems. Additionally, the Department has put in place the capability for most of the workforce to use Personal Identity Verification (PIV) cards for information system logon. Where this capability is implemented in some agencies, DOL will begin requesting use of PIV cards for information system logon. In the upcoming years, the Department will strive to achieve the full objectives of HSPD-12 by having all agencies use the PIV-based logon process. Further considerations and options for data loss prevention are also planned.

Objective 2.5: Improve electronic and information technology accessibility

[OMB Requirements: IXXB, IXXC] *Section 508 of the U.S. Rehabilitation Act* requires all federal agencies to ensure all electronic and information technology, also known and referred to as information and communication technology, is procured, developed, maintained, and made accessible to people with disabilities. The OCIO leads and coordinates with the Office of Public Affairs (OPA), the Office of Acquisition Management Services (OAMS), and the Civil Rights Center to ensure agencies comply with the Section 508 policy. The Department will be improving and enhancing its Section 508 compliance by:

- Ensuring all intranet and internet web pages are Section 508 compliant;
- Providing Section 508 compliance training to the workforce;
- Ensuring new IT investments are Section 508 compliant;
- Testing existing major IT investments for Section 508 compliance;
- Collecting metrics on mobile app accessibility testing; and
- Participating in the DHS Trusted Tester Program.

DOL has adopted the DHS Trusted Tester Program as the standard and comprehensive approach for Section 508 compliance testing of IT investments and webpages. The Department plans to implement and use the approved DHS test tools and leverage the HiSoftware Compliance Sheriff for website Section 508 compliance and reporting throughout the organization.

2.3 Goal 3 - Deliver Smarter IT

The Department understands IT is a strategic asset – critical to the day-to-day operation and effectiveness of the agencies. IT provides value in supporting and enabling the workforce to provide better, faster, and more robust services in support of business mission and goals. This better, faster, and more robust service is smarter IT delivery; and, the goal to achieve smarter IT delivery is influenced by tighter agency budgets along with the need to optimize operational efficiencies and capabilities from technology. It is also driven by the goals and objectives of the President’s Management Agenda (PMA) as well as OMB directives, initiatives, strategies (e.g. Open Data, PortfolioStat, IT Benchmarking, Cloud First, and Shared First), and FITARA. Delivering smarter IT will be achieved by focusing on the following objectives:

Objective 3.1: Enhance digital services

DOL is committed to enhancing its digital services and delivering world class customer services in alignment with OMB’s Smarter IT Delivery Cross Agency Priority (CAP) goal. In 2014, OMB developed this CAP goal to establish federal agency guidance and expectations in delivering world class customer satisfaction with high impact customer facing digital services. Federal departments are expected to implement a digital services team including digital experts, to drive the quality, effectiveness, and cost savings to high impact digital services. The team is instructed to implement cutting edge digital technologies and practices including best practices for effective digital service delivery as documented in the *Digital Services Playbook* and *TechFAR Handbook*³. The Digital Services Playbook describes key “plays” for federal agencies to deliver high impact services while the TechFAR Handbook describes the best ways agencies can implement the “plays.”

In support of OMB’s digital services initiative, the Department plans to implement a Digital Services Team (DST) which will focus on developing and establishing the DGIP capabilities, in the role of engineering and development. The DGIP scope includes three main capabilities: MDM, SDM, and application platforms. DOL has already initiated the establishment of the organizational structure of the DST; the Chief Technology Officer (CTO)/Director of Advanced Technology, who reports to the CIO, will serve as the lead. Once the DST is started, the team will identify the highest priority capabilities on which to focus.

Objective 3.2: Leverage IT shared services and establish a central management capability

[OMB Requirement: HXXC] The Department is committed to and supports the *Federal IT Shared Services Strategy* and believes in the value of implementing or utilizing IT shared services internally among agencies and externally with other federal agencies. Over the last several years, significant progress has been made in identifying IT shared service opportunities.

³ The Digital Services Playbook and TechFAR Handbook are available via the CIO Council website at: <https://cio.gov/>.

For more than ten years, DOL has been the managing partner of the Benefits.gov program, which functions as an IT shared service for information and eligibility prescreening services for more than 1,000 Federal and state benefit and assistance programs. The program is an intergovernmental, collaborative effort that partners with 17 Federal agencies, and supports four public-facing websites: Benefits.gov, GovLoans.gov, BEST.SSA.gov, and DisasterAssistance.gov.

Another example of a shared service is the electronic Capital Planning and Investment Control (eCPIC) tool. eCPIC is a GSA-operated and managed federal shared service utilized by DOL to manage its IT investment portfolio and the associated IT portfolio budget development processes. By utilizing GSA's eCPIC shared service, the OCIO reduces its operations and maintenance burden significantly. More importantly, this shared service allows the OCIO to focus its resources on higher priority CPIC program management activities instead of performing system operation and maintenance activities.

While DOL's current inventory of IT shared services demonstrate the Department's commitment to the *Federal IT Shared Services Strategy*, they are managed and operate as disparate services without a centrally managed or responsible business management function. In order to address this gap, an IT shared services approach was developed describing a program management capability, facilitating coordination across agencies and increasing the overall visibility and adoption of IT shared services. Implementation of this approach will help address some of the challenges with IT shared services being managed independently across the Department without a common set of policies, standards, processes, cost models, and performance metrics. Additionally, current IT shared services are not yet part of a centralized, consolidated services catalog where agencies can view, understand, compare, and acquire desired services. Some of the benefits anticipated from implementing a centrally managed shared services capability include consistent level of service, fewer independent acquisitions, leveraging economies of scale, and faster procurement, and provisioning. Agencies are encouraged to identify and consider other intra-IT shared service opportunities in order to leverage economies of scale and share maintenance expenses.

An IT shared services program will work in parallel with the DGIP initiative not only to promote cost efficiencies in the use of standardized software and hardware, but also to extend those benefits by allowing agencies to share common services and costs across the enterprise. By consistently having an enterprise-wide view during the early planning stages, agencies will be better positioned to adopt effective and cost efficient technologies integrated throughout the entire Department. The IT shared services program will help agencies leverage the use of DGIP capabilities.

Objective 3.3: Pursue smarter IT delivery

[OMB Requirement: HXXA] Pursuing smarter IT delivery opportunities involves identifying ways to improve how IT services and solutions are planned, acquired, and implemented for optimization. This includes adhering to the *Federal Cloud Computing Strategy* as well as seeking opportunities to implement creative and/or innovative approaches, like digital services, across the Department to deliver better, faster, smarter, and more efficient IT solutions as expected for a future-ready organization. For example, agencies need to engage internal and external customers directly to develop usable, customer-valued IT systems, services, and capabilities by utilizing open standards, a service oriented approach to architectures, and modular/incremental design principles. Smarter IT delivery also means agencies need to ensure their IT solutions are aligned to, and effectively support, the agency's business mission as well as the PMA and OMB's IT-related strategies. This approach will increase the agility and modularity of the components that comprise agency IT solutions.

In FY 2014, the OCIO implemented an enterprise-wide, cloud-based email solution which consolidated nine independent agency email systems into a single, standard Department-wide solution. The new cloud-based solution provides greater email functionality, collaboration capabilities, as well as greater file storage capacity for users.

The DGIP initiative also promotes smarter IT delivery by building a single, integrated platform to be leveraged by agencies so they can develop and deploy their IT applications. By building a single, shared IT platform, DGIP will deliver technologies and capabilities needed to support the agencies' mission IT needs and will leverage economies of scale across the Department, resulting in a sizeable savings on agency integration costs.

Objective 3.4: Improve strategic sourcing opportunities

[OMB Requirement: CXXG] The Department supports OMB's *Improving Acquisition through Strategic Sourcing Initiative* to improve and expand its use of strategic sourcing opportunities to leverage the buying power of the agencies and to reduce the duplication of commodity IT contracts. Refining the commodity IT acquisition/contracting process includes better coordination between agencies creating and/or utilizing centralized contract vehicles, and expanded negotiations with IT vendors and suppliers.

DOL recognizes the need to identify internal and external opportunities to establish Department-wide contract vehicles such as Blanket Purchase Agreements and Indefinite Delivery Indefinite Quantity contracts, as well as Enterprise License Agreements (ELA). To that end, DOL has pursued opportunities to consolidate the purchase of products utilized throughout the enterprise to take advantage of volume discounts and predetermined pricing. One example is the Microsoft Enterprise Agreement, which is an ELA constructed to consolidate the Department's software licensing and maintenance footprint for Microsoft products. Similarly, the Department has an ELA with Adobe which accomplishes the same goals, both resulting in lower service costs and a reduction in contract administration activities as well as the resources needed to manage them. Another example is the enterprise-wide mobile device and service contract currently in the planning stages but anticipated as an award to reduce the number of existing mobile contracts and to acquire

mobile devices and services using a single acquisition vehicle instead of managing hundreds of stand-alone contracts. Additionally, over the next several fiscal years, the Department will explore further opportunities for other consolidated acquisitions in the areas of operations and maintenance services; enterprise/systems/infrastructure IT engineering services; and multifunction devices such as printers/copy/faxes.

DOL also participates, where applicable, in the GSA Federal Strategic Sourcing Initiative (FSSI) program which represents a source for agencies to identify strategic sourcing opportunities, solutions, and contract vehicles for common goods and services. To support this objective, agencies are encouraged to leverage FSSI contracts to help the Department lower service and overhead administration costs and to deliver IT more efficiently and effectively. Agencies are also encouraged to established commodity IT and enterprise-wide contracts where consolidation is advantageous and provides the best value to the government.

2.4 Goal 4 - Enable the Workforce

A future-ready organization has a knowledgeable, well trained workforce equipped with the tools and technologies to successfully perform their jobs. Employing and utilizing modern technology across the Department is essential for the workforce to achieve the business mission, deliver timely program services, and provide quality customer service. Both private industry and federal government organizations are able to improve their operational effectiveness if their workforce has access to, and is able to take advantage of new technologies and associated capabilities.

The success in consolidating and enhancing the IT infrastructure, as well as delivering several modern enterprise-wide business support services, has provided the workforce a set of new tools and technology capabilities. These tools include deploying a new cloud-based HR shared service tool, a cloud-based email solution, and a modernized acquisition management system. Building on these successes, the Department plans to increase its digital and mobile computing capabilities through the DGIP initiative, a continuation of IT modernization activities enabling a future-ready workforce through the following: the unified communications initiatives including VoIP, VTC, and wireless capabilities to the national, regional, and remote offices; wireless services (MDM and MCD); records management; SDM; and a Digital Classroom solution. To meet the goal of enabling DOL's future-ready workforce, the following objectives need to be accomplished:

Objective 4.1: Promote a flexible working environment

The Department is committed to promoting a flexible working environment for its workforce. Private industry, as well as federal agencies have benefitted from an increase in workforce effectiveness by implementing flexible working environments to include flex time, teleworking, and compressed work weeks. These programs give the workforce choices they need in order to balance their careers and personal lives. Flexible working environments have been credited with increasing workforce satisfaction, decreasing

workforce absenteeism, and overall improved business performance⁴ A flexible working environment also means enabling the workforce to work from anywhere at any time – using technology. A flexible work environment is supported by the *Telework Enhancement Act of 2010* and is also promoted by DOL’s telework program which aims to enhance work/life balance, boost morale, promote productivity, and improve continuity of operations during emergencies.

A flexible working environment is facilitated by IT to allow for greater collaboration and sharing of information while working remotely or away from the traditional office location. For example, the DGIP initiative includes wireless access and wireless services to include MDM and MCD, enabling the workforce to connect and access information systems from anywhere at any time. As a fully integrated and shared service based platform, agencies will be able to fully leverage the digital and mobile capabilities offered by the DGIP initiative.

Objective 4.2: Improve learning and training opportunities

A knowledgeable and well-trained workforce will ensure the Department can perform and achieve its business mission. With the increased implementation and use of IT in performing everyday tasks, the workforce needs to keep pace with business and technology driven changes. This can be achieved through a consistent and dedicated approach to continuous learning and training. The Department supports workforce training with an online learning management system called LearningLink. LearningLink provides the workforce access to agency-specific training, human resources management, IT, accounting, and auditing training. The workforce also has access to an online library of Skillsoft training courses with over 300 business and IT related courses.

In addition to online learning opportunities, DOL recently initiated the Repository of Opportunities, Assignments, and Details program to encourage employee development through short-term, detail cross-training opportunities with other internal agencies and offices. This program enhances access to new learning opportunities via on-the-job training as well as potential new job/career opportunities and promotes and improves the agility of the workforce.

[OMB Requirement: FXXA] Through IT human capital management at DOL, agencies are committed to ensuring their workforce is future-ready by providing necessary professional development and training in support of their program’s objectives and goals. For example, the Office of the Assistant Secretary for Administration and Management (OASAM) is looking to implement a Federal Acquisition Certification for Project and Program Managers (FAC-P/PM) training program for eligible federal staff. This FAC-P/PM training program will promote the continual development of essential knowledge, skills, and abilities in order to improve project and/or program outcomes within the Department. The program will follow the guidelines established by OMB’s Office of Federal Procurement

⁴ Increase Workplace Flexibility and Boost Performance- The HBR, March 2014 <https://hbr.org/2014/03/increase-workplace-flexibility-and-boost-performance/>

Policy, but will be customized to target the challenges facing DOL program and project managers.

Furthermore, one of the technology components of the DGIP initiative is the Digital Classroom – a classroom environment integrating and leveraging technologies such as the Internet, instant messaging, web conferencing, mobile devices, classroom-specific user groups, websites, blogs, and wikis. The Digital Classroom concept will improve and enhance the learning and training experience as well as enable agencies to promote the quality and quantity of agency training along with being able to share information and content.

Objective 4.3: Encourage innovation

With rapid technology improvements comes an opportunity to leverage these changes and generate new ways of thinking to identify opportunities for improving or enhancing mission performance in areas such as: business process automation, customer service, information or idea sharing, and mobile application development. Idea sharing, collaboration, and transparency is encouraged and promoted with the Secretary’s “IdeaMill” concept. IdeaMill is the Department’s online ideation platform designed to encourage and enable the diverse workforce to submit innovative ideas for improving or enhancing the organization as a whole, as well as all the agency programs. Ideas submitted are shared, reviewed, refined and voted upon by the workforce and are implemented accordingly.

[OMB Requirement: IXXA] The Department embraces a diverse workforce and promotes an environment of inclusion through the strong relationships with over 150 local, state, and national organizations it has been able to establish and develop over the years. Through the Diversity and Inclusion Plan developed in response to *Executive Order 13583: Establishing a Coordinated Government-wide Initiative to Promote Diversity and Inclusion in the Federal Workforce*, the Department requires agencies to leverage these partnerships to increase the diversity of applicant pools and candidates, and focus on and mature these institutional relationships by establishing formal and informal partnerships. The Department recognizes its greatest asset is its diverse workforce, and will continue to embrace it while encouraging innovation and seeking new and better ways to deliver upon its mission.

Objective 4.4: Promote cybersecurity awareness

The promotion of cybersecurity awareness is imperative for the Department to maintain IT security. Providing clear, consistent, and relevant cybersecurity training and awareness communications yields the benefit of the workforce knowing what to do when confronted with a possible cyber-attack. Having knowledge and awareness of security threats reduces the risk of compromise potentially leading to data and system exposure.

DOL cybersecurity training activities include information security & awareness training, security role-based training, executive security training, privacy training, security training workshops, as well as other series-based and ad-hoc training activities. The streamlined, online role-based training program will continue to benefit the workforce and the

Department by making information system users aware of the potential risks of human error in protecting the integrity, confidentiality, and availability of information in a highly networked, systems environment. In addition to formal training, the Department will continue making opportunities to effectively communicate with the workforce about their critical role in securing DOL's information assets.

2.5 Goal 5 - Enhance IT Management

The Department looks to continuously enhance IT management in order to improve IT project management execution, strengthen cybersecurity management, have proactive disaster recovery planning, and drive IT investment performance. Federal IT projects too often fail to achieve their mission-related outcomes due to frequently incurring cost overruns and schedule slippages. An improved focus on effective IT project management and enhanced oversight will enable the delivery of more on-time, in-scope, and within budget IT projects. Strategic IT Investment Management (ITIM) will ensure the Department has the practices, policies, and processes in place to drive performance through successful planning, implementation, and the ongoing operation of IT investments.

The following objectives describe the Departments efforts to enhance IT management:

Objective 5.1: Improve IT project management execution

Efforts continue to improve IT project delivery and execution in order to increase the number of IT projects coming within 10% of budgeted costs and within 10% of planned schedule duration. Agencies are encouraged to enlist qualified IT project management professionals and to closely follow widely accepted project management practices and principles. Specifically, the Department is requiring agencies to significantly improve the practice of Earned Value Management (EVM), the federal government's standard methodology for monitoring cost, schedule, and performance of IT investments. Along with agencies improving their EVM practice, the OCIO is enhancing its IT project oversight with Program Review Board (PRB) sessions. These PRB sessions provide the OCIO greater insight and visibility into major IT projects and allow the OCIO to establish management control points for assessing project cost, schedule, and quality. PRB sessions also allow the OCIO to identify issues or problems as early as possible and take corrective action if needed. In addition to agency IT project management qualification and PRB sessions, agencies are being prompted to use IT Project Independent Validation and Verification. To assist with these efforts, the OCIO is planning an IT Program Center of Excellence.

Objective 5.2: Strengthen cybersecurity management

In response to OMB's cybersecurity memoranda on *Enhancing the Security of Federal Information and Information Systems* (M-14-03) and *Guidance on Improving Federal Information Security and Privacy Management Practices* (M-15-01), the Department released an updated Cybersecurity Program Plan (CSPP) outlining the Department's vision and strategy for achieving an enhanced and improved IT security posture. This updated CSPP serves as the Departmental cybersecurity roadmap for agencies to follow and to comply with by properly aligning cybersecurity efforts. The CSPP lays out a multi-year

strategy to strengthen cybersecurity in addition to requiring agencies to develop corresponding plans.

Objective 5.3: Have proactive disaster recovery planning

[OMB Requirement: EXXB] Federal requirements⁵ dictate that Departments have a comprehensive and effective program in place to ensure continuation of essential federal functions under all circumstances. To satisfy these federal emergency management and continuity requirements, the Department established a comprehensive Continuity Program including: detailed planning, testing, training, and exercise processes. This program ensures DOL can continue its mission of supporting the American workforce under all conditions and under a broad spectrum of emergencies.

A key component of the Continuity Program is the Department-wide Continuity Plan, which provides policy and guidance for all agencies, management components, and regional offices. Additionally, the Department has established an IT Disaster Recovery Plan (DRP), describing the policy, requirements, and plans to restore the operability of critical IT systems, applications, and/or infrastructures supporting essential business functions in response to a disaster. The IT DRP has been developed in compliance with federal policy and National Institute of Standards and Technology standards⁶, and ensures DOL has the following capabilities:

- 1) Resiliency of essential functions in an emergency;
- 2) Recovery of critical IT systems and/or network connectivity at alternate sites; and
- 3) Restoration of essential services in a timely manner as possible.

The IT DRP also describes the continuity planning activities to:

- 1) Limit the impact of IT disaster events on the Department's critical processes;
- 2) Provide detailed procedures to facilitate recovery capabilities for system owners, managers, IT experts, and other key stakeholders; and
- 3) Address the potential for long-term impacts on agencies and the Department.

The scope of the IT DRP encompasses the information systems owned and maintained by DOL as well as those operated by contract or service providers on behalf of DOL. The DOL Emergency Management Center provides Department-wide oversight and guidance for the DOL Continuity Program to ensure a viable and effective continuity capability.

⁵ Homeland Security Presidential Directive 20 (HSPD-20)/ National Security Presidential Directive 51 (NSPD-51), National Continuity Policy
⁶ Special Publication 800-34 Rev 1 Contingency Planning Guide for Federal Information Systems, May 2010, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

3 Strategic Framework

In efforts to align all of the programs, projects, and initiatives that support the aforementioned IRM SP strategic goals and objectives, DOL has developed a robust strategic framework that also serves as its IT governance process. The Department uses this process including practices and policies to ensure the efficient and effective delivery of IT services and solutions through its IT investments. The key to IT investment performance is agency adherence to this process, which aims to assist in the strategic planning, development, and implementation of IT investments and solutions that are funded to accomplish the goals and objectives of the Department's IT strategy.

[OMB Requirement: CXXA] While IT investments are managed by agencies, they are governed by the Department's IT governance structure to ensure IT investments are selected, developed, and operated efficiently and effectively. The IT governance structure guides and supports the IT investment planning process through several governance committees; one key example is the IT Acquisition Review Board (ITARB). The ITARB's mission is to ensure DOL's IT investments are managed as strategic business resources and adhere to DOL acquisition and strategic sourcing policies as well as ensuring IT investments are aligned to the Department's strategic goals. The ITARB is accountable for the approval of funds for all IT acquisitions, including infrastructure, products, commodities, and services to guarantee alignment with the Department's IT modernization and strategic sourcing initiatives. As part of the Department's budget process, agencies are required to submit IT Spend Plans that capture all planned agency IT acquisitions and map them to investments represented in the Major IT Business Case (MITBC) and IT Portfolio Summary (ITPS). These IT Spend Plans help decision making for planned IT expenditures and managing acquisition requests.

The DOL IT Governance Structure is shown below in **Figure 3** and illustrates the various functional groups and their interrelationships. The IT Capital Planning Committee (ITCPC), for example, is one of six committees led by a specific program or division within the OCIO - in this case, the ITIM Program. While each committee has a unique charter describing its roles and responsibilities, the general goal of each committee is to assist and support IT-related communications and collaboration between the OCIO and agencies. Each of the entities shown in **Figure 3** is described in greater detail in **Appendix F**.

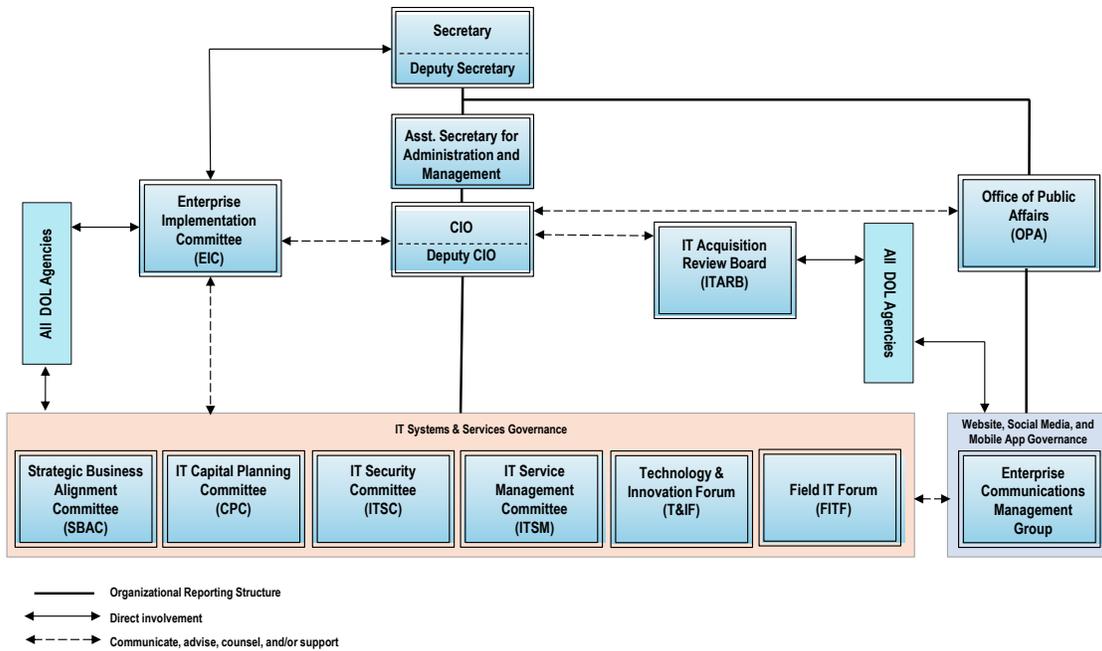


Figure 3: DOL IT Governance Structure

3.1 DOL’s Integrated IT Governance Approach

[OMB Requirement: CXXF] DOL uses an integrated IT Governance approach to strengthen IT investment management performance to ensure compliance with OMB and legislative mandates as well as align with the Department’s IT strategy. Specifically, federal agencies are required to integrate, as per the CCA and OMB, their IT Capital Planning, IT Security, and Strategic Business Management. Thus, DOL’s IT governance process incorporates the four areas described below.

IT Investment Management

Within DOL’s Division of IT Governance (DITG), the ITIM program leads the investment review processes to ensure agencies compliance with internal and federal ITIM requirements for effective and integrated IT investment management. For example, the DITG’s ITIM program office coordinates OCIO reviews of the IT components of agencies’ budget requests with the CTO, the Division of Information Assurance (DIA), and the Strategic Business Management (SBM) program. The ITIM program office also coordinates control and evaluate reviews, baseline reviews, and the MITBC/ITPS reviews by the OCIO.

DOL’s ITIM Framework provides the structural basis for specifying the alignment and integration of DOL’s SBM, CPIC, System Development Life Cycle Management (SDLCM), and IT Security management components. IT portfolio management at DOL is also managed in accordance with the ITIM Framework. **Figure 4** below illustrates DOL’s ITIM Framework with each phase described afterwards.

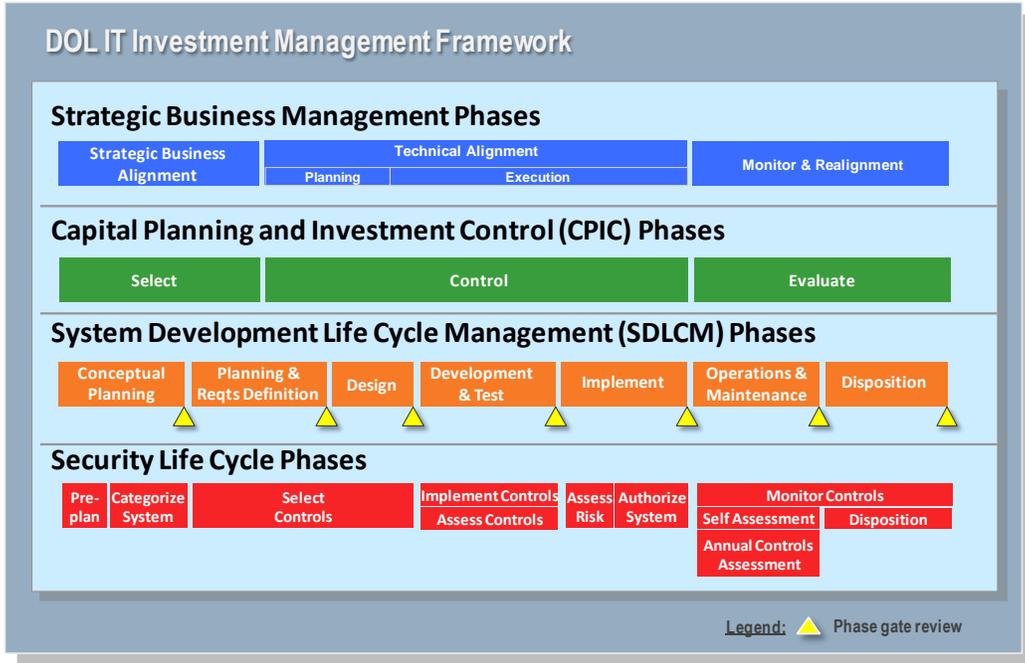


Figure 4: DOL IT Investment Management Framework

Strategic Business Management

DOL’s SBM program manages the business, performance-based and common services elements of traditional federal EA program scope. Its main focus is on improving and enhancing the alignment between business and technology across the Department to improve program performance and contribute to achieving the Secretary’s outcome goals. As with most major organizations today, IT is a key enabler to business mission success and not a business driver. As such, DOL’s OCIO continues to strategically and operationally shift its focus towards enhancing business operations and performance outcomes through implementing IT modernization initiatives, pursuing common or shared business services, and ensuring IT investments and activities are aligned, managed, and help achieve the Department’s mission.

The “Plan” stage is executed through the SBM Program, in coordination with the IT Governance process.

Plan: As part of the planning process, the DOL OCIO reviews IT strategies and outlines goals, initiatives, and activities for achieving Department IT objectives.

Capital Planning and Investment Control

DOL’s CPIC process is managed and maintained by the OCIO through a deliberate and structured approach to managing DOL’s IT investments. Agencies are directed to follow DOL’s established and highly structured CPIC process in their planning, development, acquisition, funding and budgeting of IT investments. This mature and structured CPIC process ensures a uniform approach to IT investment management at DOL. The Department’s CPIC process follows the three established phases: Select, Control, and Evaluate. Further, DOL has an

extensive resource library on CPIC guidance and performs training sessions for Departmental staff on a periodic basis.

Select: The Deputy Secretary and the Assistant Secretary for Administration and Management review specific proposed IT investments and activities and prioritize them based on how each supports the Department's strategic goals and objectives through the budget process. [OMB Requirement: CXXC] This process is informed by the Department's Strategic Plan, agency operating plans, agency priorities recommendations of the CIO and the Cost-Benefit Analysis which includes both Net Present Value and Return on Investment as evaluation criteria to comparatively evaluate IT investments. These priorities are incorporated into the Department's budget submission to OMB.

Control: Control is applied to major and non-major IT investments at the Departmental level through the CPIC processes.

[OMB Requirements: CXXD, CXXE] As part of DOL's quarterly CPIC Control phase IT investment review process, the portfolio of DOL IT investments is reviewed and assessed for policy and lifecycle process compliance with respect to each of the IT process lifecycle areas including EA. Specifically, based on threshold levels and work patterns, OCIO reviews these IT investments with respect to performance management and transition planning, including the alignment of the IT Investment with the business mission and functional needs of the agency; Agency architecture updates to capture core business functions and processes and alignment with the *Common Approach to the Federal Enterprise Architecture* including the consolidated reference models and the collaborative planning methodology. In addition, as part of the annual budget formulation process, the OCIO reviews each IT investment MITBC document to ensure the investment is aligned with the agency business mission and goals, as outlined in operating plans and the DOL's Strategic Plan.

Project plans are developed to support major IT investments identified in the agency operating plans and this Plan. The project plans and key project life cycle deliverables contain a sufficient level of detail to ensure that they satisfy requirements for achieving Departmental IT services' scope and objectives. Deliverables include those related to communications and change management, training, testing, facilities, security, contingency operations and disaster recovery.

Evaluate: A key element in evaluating the Department's IT assets is identifying performance measures for determining whether the services are delivered as they are defined and projected. Performance measures must be identified for incorporation in Service Level Agreements (SLAs) and acquisition specifications during the concept phase of the life cycle. Post-implementation service metrics are monitored to determine whether those objectives have been and continue to be achieved.

IT performance measures fall into two categories. One covers program-area-related measures considered when making investment decisions. The other addresses measures associated with the delivery of such services, including but not limited to availability, performance, reliability and functionality. The operational measures become service standards that are incorporated into SLAs and service catalogs.

System Development Life Cycle Management

DOL's SDLCM methodology is based on standard SDLC principles and practices which have proven successful for managing IT investments in both commercial and federal sectors. DOL's SDLCM is a structured mechanism to ensure IT investments are developed, modified, enhanced, as well as operated and maintained efficiently and effectively. This methodology also supports DOL's IT PMs in their planning efforts to align investments with mission goals, as well as applicable DOL IT strategic goals and critical success factors. DOL's SDLCM standardizes a repeatable, reliable, and logical process for managing IT investment development, acquisition, implementation, and operating activities to assure they are controlled, measured, documented, and ultimately improved while complying with applicable executive and legislative drivers. DOL's SDLCM adds value to IT investments by establishing a uniform and standardized approach to IT investment management while guiding DOL's IT program staff to address required activities and challenging issues throughout the IT investment life cycle.

In support of the SDLCM methodology, DOL developed the System Development Life Cycle Management Manual and serves as the mechanism to ensure IT initiatives and projects follow established and standard processes. This manual is both a standard and logical process for managing IT system development activities and acquisition approvals which can be controlled, measured, documented, and ultimately improved in accordance with the following:

- National Technology Transfer and Advancement Act of 1995
- Information Technology Management Reform Act of 1996 – ITMRA (i.e., CCA)
- OMB Circulars (i.e. A-11, A-130, A-94, A-109)

DOL's SDLCM Manual has seven phases which describe inputs, activities, and specific deliverables associated with each phase. Further, it guides DOL IT program staff on their approach which can be tailored to various types of systems development and maintenance projects.

IT Security

[OMB Requirement: EXXA] OCIO's DIA has a key role in DOL's integrated IT Governance process. Ensuring the security and privacy of information is an integral part of all phases of the CPIC process. Every phase of IT investment planning, development, implementation, operations, and disposition must incorporate security and privacy as a major concern.

The *Federal Information Security Management Act* requires agencies to integrate IT security into their capital planning and SBM processes, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to OMB. OMB Circulars A-11 and A-130 integrate IT security into the CPIC process to promote greater attention to security as a fundamental management priority. Federal agencies are required to:

- Report security costs for all information technology investments;
- Document that adequate security controls and costs have been incorporated into the life cycle planning of each investment; and
- Identify investments that support homeland security (directly and indirectly).

These and other mandates require DOL to manage and protect the information and assets that are defined by the Department's portfolio of IT investments. For more information on DOL IT security and privacy requirements and processes, consult the DOL Computer Security Handbook on LaborNet.

Some deliverables within the SDLCM are received, reviewed, and then monitored by the DIA ensuring they align with DOL's and federal IT security requirements and standards. To ensure all IT initiatives and portfolio decisions align with the Department's IT security goals, DOL continually assesses the efficiency achieved throughout the SDLCM.

APPENDIX A – OMB Requirements Matrix

The following table lists OMB requirement areas with corresponding IRM SP sections.

Code	OMB Requirement Summary	IRM SP
AXXA	Identify DOL strategic goals and objectives supported by the IRM strategic plan	Section 1.1 and Appendix B
AXXB	Describe how activities of the IRM Strategic Plan advance these goals and objectives	Section 1.1 and Appendix B
BXXA	Describe how DOL regularly evaluates existing and planned customer-facing services to measure customer use and satisfaction through analytics and other approaches	Goal 2 (obj 2.3)
BXXB	Describe how DOL regularly evaluates existing and planned customer-facing services to improve usability, availability, and accessibility of services, including optimization of services for mobile use	Goal 2 (obj 2.3)
BXXC	Describe how DOL regularly evaluates existing and planned customer-facing services to advance agency performance goals	Goal 2 (obj 2.3)
CXXA	Describe the scope of the governance process, including Investment Review Board and other Portfolio Governance Boards (as appropriate) along with delegation of authority to bureaus or other organizational units	Section 3
CXXB	Describe DOL stakeholders who are engaged, including "C"-level leadership	Appendix F
CXXC	Describe the valuation methodology used to comparatively evaluate investments, including what criteria and areas are assessed	Section 3.1
CXXD	Describe how DOL ensures investment decisions are mapped to agency goals and priorities	Section 3.1
CXXE	Provide a high-level description of the process used to assess proposed investments and make decisions, including frequency of meetings and how often the process is updated	Section 3.1
CXXF	Describe how DOL coordinates between investment decisions, portfolio management, enterprise architecture, procurement, and software development methodologies	Section 3.1
CXXG	Describe DOL's IT strategic sourcing plan, to include processes for addressing enterprise licenses	Goal 3 (obj 3.4)
DXXA	Describe how DOL policies, procedures and authorities implement CIO authorities, consistent with OMB M-11-29, "Chief Information Officer Authorities"	Appendix F
EXXA	Summarize DOL's strategy to ensuring that IT investment and portfolio decisions align with the Administration's Cybersecurity Priority Capabilities and your agency's IT security goals, and how you will continue to strengthen this alignment	Section 3.1
EXXB	Describe DOL's approach to ensure all mission critical applications have the proper continuity of operation and disaster recovery capabilities such that the agency can support the proper level of continuity of Government operations in accordance with Federal statute and guidance	Goal 5 (obj 5.3)
FXXA	Summarize DOL's approach to IT human capital planning, including the ability to build a future-ready workforce to support the agency's strategic goals and objectives	Goal 4 (obj 4.2)
GXXA	How will DOL promote interoperability and openness throughout the information life cycle? Specifically address how information collection and creation efforts, information system design, and data management and release practices will support interoperability and openness	Goal 2 (obj 2.1)
GXXB	How will DOL promote interoperability and openness throughout the information life cycle? Specifically address how DOL ensures that personal information, including personally identifiable information (PII) and controlled, unclassified information (CUI), is accessible only to authorized personnel and how frequently these controls are verified	Goal 2 (obj 2.4)
HXXA	Describe DOL's approach to maturing the IT portfolio, to include optimizing commodity IT (including data centers), rationalizing applications and adopting a service orientation approach	Goal 1 (obj 1.1) Goal 3 (obj 3.3)
HXXB	Describe DOL's plan to re-invest savings resulting from consolidations of commodity IT resources (including data centers).	Goal 1 (obj 1.1)
HXXC	Describe DOL's approach to maximizing use of inter-and intra-agency shared services	Goal 3 (obj 3.2)

Code	OMB Requirement Summary	IRM SP
	(such as those enabled by common platforms and lines of business) and shared acquisition vehicles for commodity IT, such as those determined by the Strategic Sourcing Leadership Council, in order to reduce duplicative contract vehicles.	
IXXA	Describe DOL's approach to creating a diverse environment	Goal 4 (obj 4.3)
IXXB	Describe DOL's approach to integrating accessibility considerations into IT	Goal 2 (obj 2.5)
IXXC	Describe DOL's approach to building workforce skills to support Section 508 requirements	Goal 2 (obj 2.5)

APPENDIX B – Strategic Goal Traceability

[OMB Requirement AXXA, AXXB] The Department’s Strategic Plan is the primary internal driver for the IRM SP, ensuring information resource management and resulting activities support the DOL mission. The Department’s strategic goals are listed then mapped to the supporting IT strategic goal(s) which help advance the Department strategic goal.

Strategic Goal	IT Goal 1 Modernize the IT Infrastructure	IT Goal 2 Share Information	IT Goal 3 Deliver Smarter IT	IT Goal 4 Enable the Workforce	IT Goal 5 Enhance IT Management
Department Goal 1: Prepare workers for better jobs	√	√	√	√	√
Department Goal 2: Ensure workplaces are safe and healthy	√	√	√	√	√
Department Goal 3: Promote fair & high quality work environments	√	√	√	√	√
Department Goal 4: Secure retirement, health, and other employee benefits and, for those not working, provide income security	√	√	√		
Department Goal 5: Produce timely and accurate data on the economic conditions of workers and their families		√			√

The Administration’s priorities for IT and Executive Office orders, directives, memorandums, and/or guidance were listed below then mapped to the supporting IT strategic goal(s).

Administration Priorities & Executive Mandates	IT Goal 1 Modernize the IT Infrastructure	IT Goal 2 Share Information	IT Goal 3 Deliver Smarter IT	IT Goal 4 Enable the Workforce	IT Goal 5 Enhance IT Management
Innovate					
(a) Future-Ready Workforce	NA	NA	NA	√	NA
(b) Digital Government and Open Data	NA	√	NA	NA	NA
(c) Cloud Computing	√	NA	√	NA	NA
(d) Transition to IPv6	√	NA	NA	NA	NA
Deliver: Maximizing Federal IT Value					
(a) Data Center Consolidation	√	NA	NA	NA	NA
(b) IT Shared Services	NA	NA	√	NA	NA
(c) TechStat	NA	NA	NA	NA	√
(d) PortfolioStat	√	√	√	√	√
(e) IT Dashboard	NA	NA	NA	NA	√
Protect: Advancing Cyber Security					
(a) FedRAMP	NA	NA	NA	NA	√
(b) Identity Management	NA	√	NA	NA	NA
(c) Continuous Monitoring	√	NA	NA	NA	NA
(d) Trusted Internet Connections	√	NA	NA	NA	NA
HSPD-12 (OMB M-11-11, Aug 2004)	NA	√	NA	NA	NA

Administration Priorities & Executive Mandates	IT Goal 1 Modernize the IT Infrastructure	IT Goal 2 Share Information	IT Goal 3 Deliver Smarter IT	IT Goal 4 Enable the Workforce	IT Goal 5 Enhance IT Management
Implementing IPv6 (OMB M-05-22, Aug 2005)	√	NA	NA	NA	NA
Open Government (OMB M-10-06, Dec 2006)	NA	√	NA	NA	NA
Implementing Trusted Internet Connection (OMB-08-05, Nov 2007 & M-09-32, Sept 2009)	√	NA	NA	NA	NA
Executive Order 13571 (Apr 2011)	NA	√	NA	NA	NA
Implementing EO 13571 (OMB M-11-24, June 2011)	NA	√	NA	NA	NA
CIO Responsibilities (OMB M-11-29, Aug 2011)	NA	NA	NA	NA	√
Performance Management (OMB M-11-31, Aug 2011)	NA	NA	NA	NA	NA
Implementing PortfolioStat (OMB M-12-10, Mar 2012)	√	√	√	√	√
Strategic Sourcing (OMB M-13-02, Dec 2012)	NA	NA	√	NA	NA
Managing Government Records (OMB M-12-18, Aug 2012)	NA	√	NA	NA	NA
Implementing PortfolioStat FY 2013 Guidance (OMB M-13-1309, Mar 2013)	√	√	√	√	√
Executive Order- Making Open and Machine Readable the New Default for Government Information, May 2013	NA	√	NA	NA	NA
Open Data Policy – Managing Information as an Asset (OMB M-13-13, May 2013)	NA	√	NA	NA	√
Enhancing Security of Federal Information and Systems (OMB M-14-03, Nov 2013)	NA	NA	NA	NA	√
Second Open Government National Action Plan, Dec 2013	NA	√	NA	NA	NA
Revisions to the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM), Dec 2013	NA	NA	NA	NA	√
FY 2014 PortfolioStat Guidance (OMB M-14-08, May 2014)	√	√	√	√	√
Executive Order 13673-Fair Pay and Safe Workplaces, July 2014	NA	√	NA	NA	NA
Management Agenda Priorities for the FY 2016 Budget (OMB M-14-12, July 2014)	√	√	√	√	√
Guidance on Managing Email (OMB M-14-16, Sept 2014)	NA	√	NA	NA	NA
FY 2015 Guidance on Improving Federal Information Security and Privacy Management Practices (OMB M-15-01, Oct 2014)	NA	NA	NA	NA	√

APPENDIX C – IRM SP Update Process

This document was updated leveraging both internal and external inputs and followed the process illustrated below in **Figure 5**.

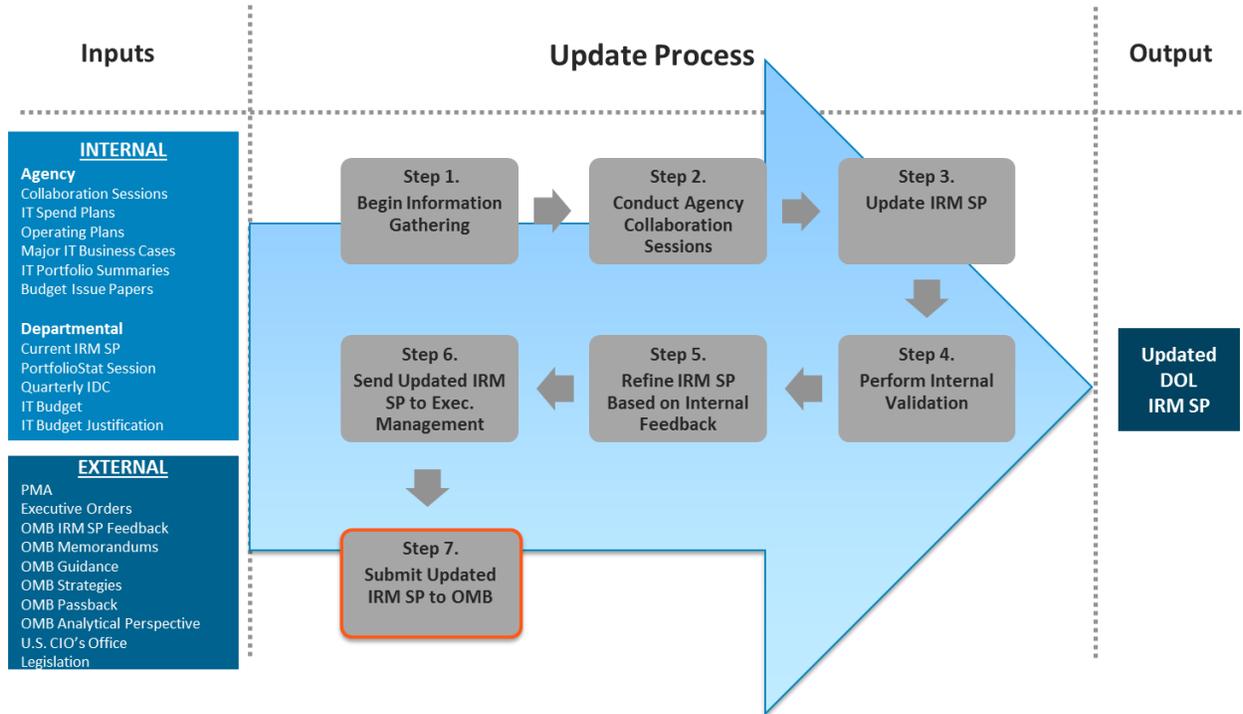


Figure 5: IRM SP Update Process

- Step 1: Information gathering begins after submitting the IRM SP to OMB. This is a year-around, continuous activity.
- Step 2: Collaboration sessions are held with key business managers, stakeholders, and IT managers of the agencies to understand near and longer term IT priorities and strategies.
- Step 3: Updates are made to the IRM SP reflecting changes to or new internal and external inputs.
- Step 4: The updated IRM SP is sent to Sr. OCIO staff and the agencies (through the EIC members) for validation (review, comment, and feedback).
- Step 5: The IRM SP is refined after internal validation.
- Step 6: The validated IRM SP is sent to Executive Management for review and clearance.
- Step 7: DOL's updated IRM SP is submitted to OMB and posted to Dol.gov.

APPENDIX D – Departmental Drivers

The update of this IRM SP was informed and guided by a number of Departmental drivers (i.e., internal data inputs). The columns below represent agency-level, OCIO-level, and Department-level resources or data inputs for this IRM SP.

Agency	OCIO	Department
Collaboration Sessions & Report	Collaboration Sessions	Vision
Operating Plans	IT Modernization Program	Mission
IT Strategic Plans	IT Modernization Master Schedule	Strategic Goals
Major IT Business Case(s)	Major IT Business Case(s)	FY 2014 PortfolioStat session materials from OMB
IT Portfolio Summaries	IT Modernization Communications	FY 2016 IT Budget Passback from OMB
Performance Budget Issue Papers	CIO Communications	FY 2016 Congressional Budget Justification for IT Modernization
	OCIO All Hands Meetings	Customer Service Program
		FY 2015 IT Budget Constraints

APPENDIX E – Governmental Drivers

The update of this IRM SP was informed and guided by a number of Governmental drivers (i.e., external data inputs) from the Executive Office of the President (left column of the table below) or Congressional Legislation (right column of the table below) relating to information resources management.

Executive Office	Legislation
Administration Priorities for federal IT ⁷	Clinger Cohen Act (CCA) of 1996
Presidential Decision Directive 63	Chief Financial Officers Act of 1990
Chief Information Officers (CIO) Council	Government Performance and Results Act (GPRA) of 1993
OMB A-11, A-130, A-94	Government Management Reform Act (GMRA) of 1994
President’s Memorandum on Transparency and Open Government, Jan 2009	Federal Acquisition Streamlining Act
M-10-06 Open Government, Dec 2009	Federal Acquisition Reform Act
The 25 Point Implementation Plan to Reform Federal Information Technology Management, Dec 2010	Government Paperwork Elimination Act (GPEA) of 1998
The Federal Cloud Computing Strategy, Feb 2011	Paperwork Reduction Act (PRA) of 1995
M-11-29 CIO Responsibilities, Aug 2011	Federal Information Security Management Act (FISMA)
E.O. 13571 Streamlining Service Delivery and Improving Customer Service, Apr 2011	Federal Financial Management Improvement Act
E.O. 13576 Delivering an Efficient, Effective, and Accountable Government, June 2011	National Technology Transfer and Advancement Act of 1995
M-11-31 Effective, Efficient, and Accountable Government, Aug 2011	Section 508, Rehabilitation Act of 1998
M-12-10 Implementing PortfolioStat, Mar 2012	E-Government Act of 2002
The Federal IT Shared Services Strategy, May 2012	Telework Enhancement Act of 2010
M-12-13 FY14 Budget Guidance, May 2012	Presidential and Federal Records Act Amendments of 2014
The Common Approach to Federal Enterprise Architecture, May 2012	Digital Accountability and Transparency Act of 2014
The Federal Digital Government Strategy, May 2012	Federal Information Technology Acquisition Reform Act of 2015
M-12-18 Managing Government Records, Aug 2012	
M-13-02 Improving Strategic Sourcing, Dec 2012	
M-13-09 FY 2013 PortfolioStat Guidance, Mar 2013	
E.O. Making Open and Machine Readable the New Default for Government Information, Mar 2013	
M-13-13 Open Data Policy – Managing Information as an Asset, May 2013	
M-14-03 Enhancing Security of Federal Information Systems, Nov 2013	
Second Open Government National Action Plan, Dec 2013	
M-14-08 FY14 PortfolioStat Guidance, Mar 2014	
E.O. 13673 Fair Pay and Safe Workplaces, July 2014	
M-14-12 President’s Management Agenda for FY16, July 2014	
M-14-16 Guidance on Managing Email, Sept 2014	
M-15-01 Improving Information Security & Privacy, Oct 2014	
M-15-12 Increasing Transparency of Federal Spending by Making Data Accessible, Searchable, and Reliable, May 2015	

⁷ U.S. CIO’s Agenda, available at <https://cio.gov/agenda/>

APPENDIX F – IT Governance Structure

DOL’s IT Governance Structure represents an organizational leadership and decision making process with the goal of ensuring IT investments are selected, developed, and operated efficiently and effectively in support of the business mission and strategic IT direction.

DOL OCIO

The OCIO, led by the CIO, has the lead role in most of the IT governance activities shown in **Figure 3** (see Section 3) including senior management (top-down) reviews as well as bottom-up review and analysis of IT investment performance and portfolio management. For agency IT investment Project Managers (PMs), the OCIO is a valuable source of IT investment management information. This includes providing IT investment guidance, resources, and standardized project management templates, and methodologies to assist PMs with managing and delivering successful IT investments.

The OCIO is the key organization for the implementation of the CPIC process as it:

- Leads the review and management oversight of IT investments;
- Makes recommendations to approve candidate initiatives for inclusion in the Department’s portfolio of IT investments;
- Oversees and manages the Department’s implementation of the Select–Control–Evaluate phases; and
- Works with agencies to promote effective IT investment management and performance.

[OMB Requirement: DXXA] DOL has designated a CIO whose primary responsibility is to manage the Department’s information resources. Consistent with OMB’s Memorandum on *Chief Information Officer Authorities* (M-11-29) and FITARA, the CIO has the authority and lead performance role in the following four areas: governance, commodity IT, program management, and information security. With the responsibility in these four areas, the CIO is held accountable for lowering operational costs, terminating and turning around troubled IT projects, and delivering meaningful functionality while enhancing the security of information systems. These authorities also enable the CIO to reduce the number of duplicative systems, simplify services for American citizens, and deliver more effective IT to support DOL's mission.

In addition to the above, the CIO is required to implement:

- A Department-wide capital planning and investment control (CPIC) process to ensure effective and efficient management of DOL’s portfolio of IT investments; and
- A Department-wide records management process to ensure the effective capture, preservation, management, and disposal of electronic records.

DOL Executive Leadership

[OMB Requirement: CXXB] DOL’s executive leadership determines the annual budget requests including requests for funding new and ongoing IT investments. Executive leadership includes the Secretary and Deputy Secretary of Labor with input from Departmental Budget Center, the Center for Program Performance and Results, the Office of the Chief Financial Officer (OCFO),

and the OCIO. Executive leadership ensures the Department’s IT portfolio continues to support the Department’s mission, goals, and business objectives.

Enterprise Implementation Committee

The Enterprise Implementation Committee (EIC) is a senior management-level panel which provides planning input and operational review of enterprise-wide IT initiatives. The EIC supports the use of IT to meet business objectives, increase collaboration and best practices between agencies, ensure IT performance, and promote innovation. The EIC is chaired by the Deputy Secretary. Its members include senior agency business executives.

IT Acquisition Review Board

The ITARB is tasked with reviewing and approving planned IT acquisitions including purchases, procurements, and/or contracts in order to reduce costs, avoid duplication, and pursue strategic sourcing opportunities. The ITARB supports requirements for the effective use of DOL’s IT budget.

IT Governance Bodies

There are six committees and forums that provide management and technical advice, council and support to DOL’s IT governance process. They include the Strategic Business Alignment Committee (SBAC), IT Capital Planning Committee (CPC), IT Security Committee (ITSC), Technology and Innovation Forum (T&IF), Field IT Forum (FITF), and IT Service Management Committee (ITSMC). **Table 1** below lists and provides a brief description and the participants of DOL’s IT Governance Bodies as part of DOL’s IT Governance Structure.

Table 1: DOL IT Governance Bodies

Body	Description	Participants
EIC	The EIC’s mission is to ensure all initiatives affecting IT infrastructure, common services and customer service programs having cross-agency impacts are implemented to provide effective support for the Department’s business mission and operations.	<ul style="list-style-type: none"> • Deputy Secretary, Chair; • CIO, Vice-Chair; • Deputy CIO; • Chief Financial Officer (CFO); • One member authorized to speak for the Agency from the following: BLS, EBSA, ETA, MSHA, OSHA, OALJ, OASAM, ODEP, OFCCP, OIG, OPA, SOL, OWCP, VETS, WHD; • One small Agency representative drawn from ILAB, OAS, OLMS, OSBP, WB; and • 3 members appointed from region/field
ITARB	The ITARB’s mission is to ensure Department and Agency IT acquisitions are managed as strategic business resources, and adhere to Department acquisition and strategic sourcing policies.	<ul style="list-style-type: none"> • CIO, Chair; • Deputy CIO, Vice Chair; • Chief Technology Officer (CTO); • Director, IT Governance; and • Director, OAMS
SBAC	The SBAC’s mission will be to ensure Department and Agency planning activities, strategic business goals, and operating plans	<ul style="list-style-type: none"> • Director, IT Governance, Chair; and • One business representative responsible for strategic planning & an alternate from each DOL Agency or Office: BLS, EBSA, ETA, MSHA,

Body	Description	Participants
	are aligned with Department-wide initiatives and managed as strategic business resources.	OSHA, OASAM, OCFO, OFCCP, OIG, OLMS, OPA, OWCP, WHD, OALJ, ODEP, SOL, VETS <ul style="list-style-type: none"> • Small Agency representatives participate as interested and upon request.
CPC	The CPC’s mission is to ensure compliance with federal and departmental CPIC policy, regulations and controls so DOL IT investments achieve their intended results on time and within budget.	<ul style="list-style-type: none"> • CPIC Program Manager, Chair; • One member authorized to speak for the Agency from the following: BLS, EBSA, ETA, MSHA, OALJ, OASAM, OASP, OCFO, ODEP, OFCCP, OLMS, OPA, OSHA, OWCP, SOL, WHD, the Adjudicatory Boards; and • One small Agency representative.
ITSC	The ITSC’s mission is to define and develop IT security policies and procedures, promulgating them within their Agency.	<ul style="list-style-type: none"> • Chief Information Security Officer (CISO), Chair; • One technical, security representative and an alternate from each of the following Agencies: BLS, EBSA, ETA, MSHA, OSHA, OALJ, OASAM, OCFO, OFCCP, OIG, OLMS, OPA, SOL, OWCP, VETS, WHD; and • Small Agency representatives participate as interested and upon request.
T&IF	The T&IF’s mission is to foster collaboration and ideation processes; empower staff and customers to share ideas; identify and test entrepreneurial and innovative technology; and create an environment where staff and customers contribute technology solutions to support the Department’s mission.	<ul style="list-style-type: none"> • CTO, Chair; • Agency infrastructure owners; • Agency systems owners; and • Agency enterprise application owners.
FITF	The FITF’s will raise awareness, understanding, acceptance, and ownership of DOL’s IT Modernization initiatives among field stakeholders throughout the Department and Agencies.	<ul style="list-style-type: none"> • Associate Deputy CIO, Chair; • Agency infrastructure owners; • Agency systems owners; and • Agency enterprise application owners.
ITSMC	The ITSMC’s mission is to define, implement and oversee IT service management and change management processes, and manage risks to ensure the integrity of DOL enterprise systems shared across two or more Agencies.	<ul style="list-style-type: none"> • Director of the Enterprise Service Office (ESO), Chair; • Agency infrastructure owners; • Agency systems owners; and • Agency enterprise application owners.

APPENDIX G – List of Acronyms

Acronym	Definition
API	Application Programming Interface
BLS	Bureau of Labor and Statistics
CAP	Cross Agency Priority
CCA	Clinger-Cohen Act of 1996
CIO	Chief Information Officer
CPC	Capital Planning Committee
CPIC	Capital Planning and Investment Control
CRM	Customer Relationship Management
CSPO	Customer Service Program Office
CSPP	Cyber Security Program Plan
CTO	Chief Technology Officer
DATA Act	Digital Accountability and Transparency Act of 2014
DHS	U.S. Department of Homeland Security
Department	U.S. Department of Labor
DGIP	Digital Government Integrated Platform
DIA	Division of Information Assurance
DITG	Division of Information Technology Governance
DOL	U.S. Department of Labor
DRP	Disaster Recovery Plan
DST	Digital Services Team
EA	Enterprise Architecture
EBSA	Employee Benefits Security Administration
eCPIC	Electronic Capital Planning and Investment Control
EIC	Enterprise Implementation Committee
ELA	Enterprise License Agreement
ETA	Employment and Training Administration
EVM	Earned Value Management
FAC-P/PM	Federal Acquisition Certification for Project and Program Managers
FITARA	Federal Information Technology Acquisition Reform Act
FITF	Field Information Technology Forum
FSSI	Federal Strategic Sourcing Initiative
FY	Fiscal Year
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
IPv6	Internet Protocol Version 6.0
IRM SP	Information Resources Management Strategic Plan
IT	Information Technology
ITARB	Information Technology Acquisition Review Board
ITCPC	Information Technology Capital Planning Committee
ITIM	Information Technology Investment Management
ITPS	Information Technology Portfolio Summary
ITSC	Information Technology Security Committee
ITSMC	Information Technology Service Management Committee

Acronym	Definition
MCD	Mobile Content Delivery
MDM	Mobile Device Management
MITBC	Major Information Technology Business Case
MSHA	Mine Safety and Health Administration
NARA	National Archives and Records Administration
OALJ	Office of Administrative Law Judges
OAMS	Office of Acquisition Management Services
OASAM	Office of the Assistant Secretary of Administration and Management
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OData	Open Data Protocol
OFCCP	Office of Federal Contract Compliance Programs
OIG	Office of the Inspector General
OMB	U.S. Office of Management and Budget
OPA	Office of Public Affairs
OSHA	Occupational Safety and Health Administration
PIV	Personal Identity Verification
PM	Project Management
PMA	Presidents Management Agenda
PRB	Program Review Board
SBAC	Strategic Business Alignment Committee
SBM	Strategic Business Management
SDLCM	System Development Life Cycle Management
SDM	Strategic Data Management
SMART	Secretarial Management and Records Tracking
SLA	Service Level Agreement
SOC	Security Operations Center
TIC	Trusted Internet Connection
T&IF	Technology and Innovation Forum
VoIP	Voice Over Internet Protocol
VTC	Video Conferencing
WHD	Wage and Hour Division

