

U.S. Department of Labor

Office of Inspector General—Office of Audit

**REPORT TO THE OFFICE OF THE
DEPUTY SECRETARY**



**DOL'S IT GOVERNANCE LACKED THE
FRAMEWORK NECESSARY TO
SUPPORT THE OVERALL MISSION**

**DATE ISSUED: SEPTEMBER 30, 2021
REPORT NUMBER: 23-21-002-01-001**



BRIEFLY...

DOL'S IT GOVERNANCE LACKED THE FRAMEWORK NECESSARY TO SUPPORT THE OVERALL MISSION

September 30, 2021

WHY OIG CONDUCTED THE AUDIT

The Department of Labor (DOL) spends over \$685 million annually on a portfolio of information technology (IT) assets that support the operation and management of its programs. Prior audit work found DOL's information security program contained deficiencies in critical, high-risk areas. As cited for many years through our previous audit reports, these issues were attributed, in part, to the DOL Chief Information Officer's (CIO) lack of authority and a misaligned reporting structure.

WHAT OIG DID

We conducted a performance audit to determine:

Whether DOL's IT governance structure appropriately aligns authority and responsibility to support the overall mission of the Department.

To answer our objective, we interviewed senior DOL leadership, evaluated documents related to IT governance and operations, and surveyed DOL agency staff and leadership. We also interviewed CIOs from other federal agencies for benchmarking purposes.

READ THE FULL REPORT

<http://www.oig.dol.gov/public/reports/oa/2021/23-21-002-01-001.pdf>

WHAT OIG FOUND

Based on the results of our audit work, we determined DOL's IT governance structure does not appropriately align authority and responsibility to support the overall mission of DOL. We found IT governance at DOL was ambiguous, ad hoc, and reliant on personnel to fulfill their duties without codified policies and procedures.

To be effective, a CIO must be organizationally positioned within leadership to ensure the implementation of IT Governance without the appearance of any conflicts of interest. This is not the case at DOL, as the CIO reports to the ASAM, the head of one of the CIO's customer agency, who also represents the CIO in key enterprise planning and strategy meetings.

While DOL made progress in ensuring the CIO controls key IT elements within the department, blind spots remain. The CIO remains impaired in visibility and authority over DOL IT within agencies not fully integrating into the IT Shared Services model.

The DOL's IT processes critical to proper IT governance were weakened by ad hoc design and reliance upon personnel. Additionally, with the recent transition to IT Shared Services, the absence of clearly documented requirements and processes created confusion among agencies dependent upon OCIO for IT support.

As a result, the current state of DOL IT is reliant upon the direction of the ASAM and, without implementing codified structures, it is directly impacted by the changing of personnel.

WHAT OIG RECOMMENDED

We made five recommendations to the Deputy Secretary of Labor to improve DOL's establishment and implementation of IT governance across the enterprise. The Associate Deputy Secretary for the Department disagreed with one recommendation to provide the CIO with the authority, accountability, and independence required to effectively manage the Department's IT by elevating the CIO to a level commensurate with the DOL's Assistant Secretaries and the Chief Financial Officer and reporting to the Deputy Secretary. The other four recommendations were accepted.

TABLE OF CONTENTS

INSPECTOR GENERAL’S REPORT	1
BACKGROUND	3
RESULTS	10
Alignment of CIO Limits Enterprise Level Visibility and Authority	11
Blind Spots Existed in IT Governance Across DOL Agencies	20
Key IT Governance Elements Remained Ambiguous Due to Ad Hoc Execution	23
CONCLUSION	27
OIG’S RECOMMENDATIONS	28
Summary of the Department’s Response	28
EXHIBIT 1: CUSTOMER AGENCIES OF OCIO PRIOR TO IT SHARED SERVICES	30
EXHIBIT 2: CUSTOMER AGENCIES OF OCIO UNDER IT SHARED SERVICES	31
APPENDIX A: SCOPE, METHODOLOGY, & CRITERIA	32
APPENDIX B: AGENCY’S RESPONSE TO THE REPORT	34
APPENDIX C: ACKNOWLEDGEMENTS	39

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210



INSPECTOR GENERAL'S REPORT

Julie A. Su
Deputy Secretary of Labor
U.S. Department of Labor
200 Constitution Ave, NW
Washington, DC 20210

This report presents the results of our audit of the Department of Labor's (DOL) IT governance. The information provides our insight on DOL's IT governance structure and operations for your consideration as you implement your vision.

DOL spends over \$685 million annually on a portfolio of information technology (IT) assets that support the operation and management of its programs. Prior audit work found DOL's information security program to contain deficiencies in critical, high-risk areas. As cited for many years through previous Office of Inspector General (OIG) audit reports, these issues were attributed, in part, to the DOL Chief Information Officer's (CIO) lack of authority and a misaligned reporting structure, as the CIO has not been elevated to an adequate level to carry out required duties as mandated by law and Executive Branch guidance.

In 2019, DOL began undergoing an effort under the direction of the Assistant Secretary for Administration and Management (ASAM) that significantly changed the way DOL provides IT services in support of agency missions. Specifically, DOL realigned its IT resources from across the organization, consolidating IT functions into an IT Shared Services model. To accomplish this DOL moved operations and management of its IT, along with moving the majority of information technology specialists from the agencies to the Office of the Assistant Secretary for Administration and Management (OASAM), under the direction of the CIO.

Given our prior concerns and the changes underway, we conducted an audit to determine:

Whether DOL's IT governance structure appropriately aligns authority and responsibility to support the overall mission of the Department.

To answer our objective, we interviewed senior DOL leadership, reviewed documents related to IT governance and operations, and surveyed DOL agencies and leadership. We also interviewed CIOs from other federal agencies to understand how their respective agencies implemented IT governance.

Based on the results of our audit work, we determined DOL's IT governance structure does not appropriately align authority and responsibility to support the overall mission of DOL. We found IT governance at DOL was ambiguous, ad hoc, and reliant on personnel to fulfill their duties without codified policies and procedures. In addition, to be effective, a CIO must be organizationally positioned within leadership to ensure the implementation of IT governance without the appearance of any conflicts of interest; however, this is not the case at DOL. DOL made progress in ensuring OASAM and the Office of the Chief Information Officer (OCIO) control key functions, including IT, within the Department. However, blind spots remained in their visibility and authority over IT due to agencies not fully integrating into IT Shared Services. Additionally, DOL's IT processes critical to proper IT governance were weakened by ad hoc design and reliance upon personnel. As a result, the current state of DOL IT is reliant upon the direction of the ASAM and without implementing codified structures; it is directly impacted by the changing of personnel.

The Associate Deputy Secretary disagreed with the information and conclusions in our report and provided unofficial and official responses. We reviewed the information provided and made changes as appropriate. We determined some of the information provided in the responses was outside of our audit scope, not complete, or did not contain sufficient support to change our conclusions and recommendations. For example, the responses requested highlighting the Department's improvements in the Federal Information Technology Acquisition Reform Act (FITARA) scorecard,¹ as the Department scored mainly "A" grades. However, the responses failed to mention that the overall score was a "B-" due to the Department being only one of the three remaining 24 CFO Act agencies to answer "No" to having the CIO reporting to the Secretary or Deputy Secretary. Additionally, the responses highlighted the closing of OIG recommendations as a significant accomplishment; however, we remain concerned that significant IT management recommendations have been unaddressed for years including concerns related to IT inventory weaknesses.

¹ The FITARA scorecard is a metric of federal agency compliance with FITARA requirements.

BACKGROUND

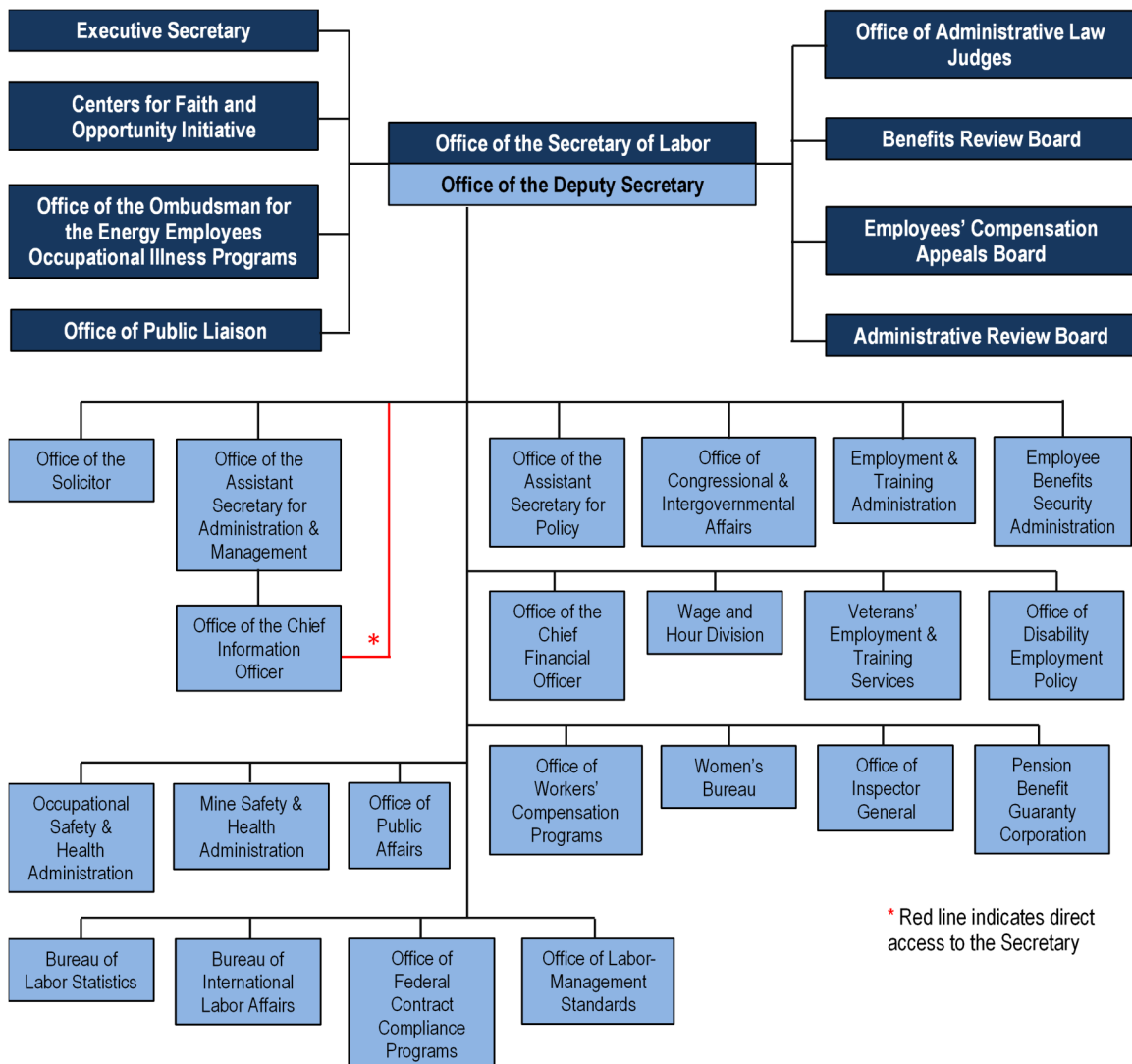
IT governance is the authority a CIO executes through their leadership, organizational structure, and processes that is linked to enterprise governance strategy and ensures all IT assets support the enterprise mission. An effective IT governance structure is critical to ensure that DOL's IT spending is properly managed, IT security for DOL's infrastructure is maintained, IT policies and procedures are consistently applied, and the confidentiality of DOL's information is protected. Key elements of IT governance include spending, procurement, client engagement, asset inventory, and system ownership. A sound IT governance implementation will protect the integrity of DOL's data and ensure the availability of critical DOL resources to the American public.

To understand IT governance at DOL, we examined the organizational structure of the Department, specifically, OCIO, the implementation of IT Shared Services, and DOL's IT governance structure, as established.

DOL'S IT ORGANIZATIONAL STRUCTURE

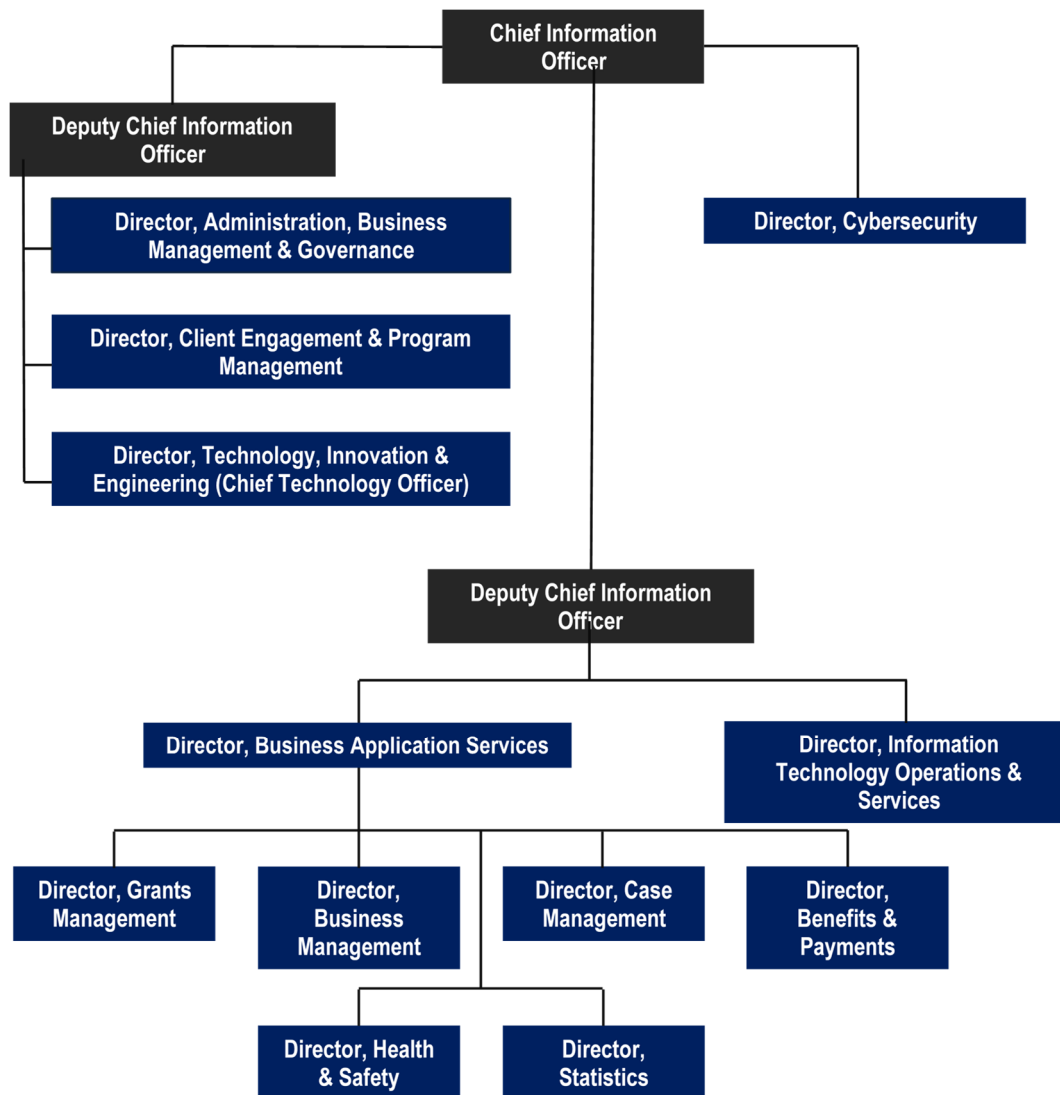
At DOL, the CIO reports to the ASAM in performing the duties required to provide IT services for the Department and its agencies. The OCIO is one of the many programs and offices located within OASAM. OASAM is 1 of 21 agencies that report to the Deputy Secretary of Labor, as seen in Figure 1.

Figure 1: DOL Organizational Chart



Source: DOL Public Webpage

In leading DOL's information technology, the CIO oversees 6 directorates, consisting of 341 federal employees and 1310 contract staff. The CIO is supported by two Deputy CIOs and a Director of Cybersecurity, as seen in Figure 2.

Figure 2: High-Level OCIO Organizational Chart

Source: OCIO

One Deputy CIO oversees three Directorates: (1) Administration, Business Management and Governance, (2) Client Engagement and Program Management, and (3) Technology, Innovation and Engineering. The Directorate of Administration, Business Management and Governance is responsible for providing a clear orientation and direction for OCIO staff on all administrative, financial, procurement and governance matters. The Directorate for Client Engagement and Program Management is responsible for overseeing engagement with OCIO clients to understand the functional and technical issues that the client faces and communicating these issues to the appropriate parties in OCIO as well as all aspects of project and portfolio management to ensure that

OCIO projects meet their desired outcomes. Finally, the Directorate for Technology, Innovation, and Engineering is responsible for developing and maintaining DOL's long-term enterprise IT strategic plans and enterprise architecture along with improving delivered system performance.

The second Deputy CIO oversees two Directorates: (1) Business Application Services and (2) Information Technology Operations and Services. The Directorate of Business Application Services manages all business-focused projects throughout the development life cycle, including staff resources and the utilization and performance of the business-focused application portfolio. The Directorate of Information Technology Operations and Services provides enterprise-wide IT infrastructure and cloud resources, monitors all aspects of the DOL network, implements and maintains enterprise and agency applications, and manages the Enterprise Service Desk.

DOL's Chief Information Security Officer (CISO) is responsible for managing the Department-wide cyber security program and supports DOL's mission by promoting and bolstering enterprise-level cybersecurity defenses and ensuring that the Department's program operates effectively. The CISO's primary objective is to ensure the confidentiality, integrity, and availability of DOL information and information systems.

IT SHARED SERVICES

In 2018, DOL management communicated its goal to optimize the Department's enterprise services in line with the Presidential Management Agenda and Executive Order 13781, the latter of which mandates each federal agency enhance the efficiency and effectiveness of administrative services. The Enterprise-wide Shared Services (ESS) initiative focused on improving administrative efficiency and effectiveness by centralizing disparate administrative functions (HR, IT, Procurement, and Personnel Security) throughout DOL mission agencies and reorganizing them under their corresponding centralized office to ensure proper oversight and consistency in service. The ESS initiative was organized, executed, and overseen by OASAM at the direction of the ASAM.

As a part of the ESS initiative, DOL's IT Shared Services effort involved transitioning the accountability, authority, and operations of IT from the agencies to a central authority within OASAM, the CIO. Additionally, DOL management transferred IT-related staff positions within agencies to OASAM's OCIO, including IT Specialists and other positions that support IT work, such as Contracting Officer Representatives and Project Managers of IT-related procurements. Five agencies were already fully reliant upon OASAM's OCIO for their IT services

prior to the creation of IT Shared Services, while others were set to transition under this new initiative (see Exhibit 1 for full listing). All DOL agencies incorporated as part of the IT Shared Services initiative signed Memorandums of Understanding (MOU) between agency leadership and the ASAM to define IT roles and service level requirements.

Initial planning for IT Shared Services included transferring IT operations and responsibilities of all 18 DOL agencies to the OASAM's OCIO.² The transition began with one agency as a pilot in October 2019, and, as of January 2021, the majority of DOL's agencies had transitioned into IT Shared Services (see Exhibit 2 for full listing).³ While the Department initially planned to incorporate the Bureau of Labor Statistics (BLS) and Office of the Chief Financial Officer (OCFO) into IT Shared Services by the end of Fiscal Year 2020, these two agencies have since been removed from any timeline of planned agency transitions under the initiative.

RESTRUCTURING OF IT GOVERNANCE AT DOL

With this major initiative to transform DOL's decentralized IT management and operations and shift to an IT Shared Services model, the Department's IT governance structure necessitated changes. To this end, DOL changed the authority and accountability of all IT to reside with the CIO, under the ASAM. Under this new structure, three review boards were created and approved by the ASAM to govern IT investments, enterprise architecture, and IT performance.

IT GOVERNANCE BOARDS

DOL's IT governance boards consist of the Investment Review Board (IRB), the Enterprise Architecture Review Board (EARB), and the IT Performance Review Board (PRB). The IRB, EARB, and PRB consist of membership from DOL agencies. Agencies that do not have an active member on the board are represented by another agency's member. BLS and OCFO, while not integrated into IT Shared Services, are members of all three boards and their IT Investments and projects go through the boards in the similar fashion to the other agencies.⁴ The overall focus of these three boards is on the management of IT

² The Department intentionally excluded the OIG from IT Shared Services due to independence requirements of the Inspector General Act of 1978.

³ As of June 2021, ETA Job Corps was still in the process of moving into IT Shared Services. In addition, the Department excluded elements of MSHA - Mine Emergency Operations (MEO) and District IT from IT Shared Services given their specialized role in mine operations.

⁴ The OIG is not a member of these boards.

projects and investments; however, the actual funding approval is handled via annual IT Spend Plans and the IT Acquisition Review Board (ITARB). While these boards give the agencies a forum to provide input, these boards do not directly engage with the Secretary or Deputy Secretary.

Investment Review Board (IRB)

In July 2019, board members adopted the IRB charter, establishing the IRB as the highest level IT governance board at DOL. The IRB governs the Department's existing and proposed IT services, investments, programs, initiatives, and resources. All members of the board must be DOL senior executives who are authorized to speak on the behalf of their respective agency. This is the only board chaired by the CIO and identifies specific agency membership. Per the charter, the board also consists of the Chief Financial Officer, ASAM, a representative from the Office of the Secretary (OSEC)⁵, OASAM Deputy Assistant Secretary for Budget and the head or career deputy (or designee) from the following agencies:

- Bureau of Labor Statistics (BLS)
- Employee Benefits Security Administration (EBSA)
- Employment and Training Administration (ETA)
- Mine Safety and Health Administration (MSHA)
- Office of Federal Contract Compliance Programs (OFCCP)
- Occupational Safety and Health Administration (OSHA)
- Office of Workers' Compensation Programs (OWCP)
- Wage and Hour Division (WHD)
- Small Agency⁶ (2 rotating members)

The board meets bi-monthly and is responsible for reviewing proposed IT investments and making recommendations for funding. The board reviews both new and modified IT investment proposals and is responsible for ensuring transparency when working with agencies. While recommendations for investment approval are made by the IRB, actual funding approval is handled via annual IT Spend Plans and the ITARB.

Enterprise Architecture Review Board (EARB)

In February 2020, board members adopted the EARB charter, establishing what is considered a collaborative forum that serves as an advisory board to the IRB. The board is responsible for identifying existing applications, processes, and technologies within the Department to leverage prior to looking externally for

⁵ A review of the meeting minutes during FY20 indicated the OSEC representative who attended was neither the Secretary nor the Deputy Secretary.

⁶ Small agencies are defined as having an IT investment portfolio less than \$10 million.

solutions. This advisory board allows agencies the opportunity to understand whether other agencies are experiencing similar issues or must meet the same requirements and to discuss common solutions and best practices.

The charter specified that the members of this board consist of a rotating Business Product Owner (BPO) as the Chair and the Chief Technology Officer (CTO) as the Co-Chair. Other members of the board include the Deputy Chief Information Officer⁷, Chief Information Security Officer (or designee), Director of IT Budget and Finance Management⁸, Business Product Owner(s), IT Service Owner(s), IT Division Director(s) as needed, IT Program Manager/Investment Owner, and Subject Matter Expert(s). While all members must be DOL federal employees and authorized to speak on behalf of their agencies, the EARB's charter does not identify the specific agencies required to attend. The board is to meet twice a month to review proposed, new, and existing enterprise-wide and agency-specific IT investments from an architectural standpoint.

IT Performance Review Board (PRB)

In March 2020, board members formally adopted the PRB charter, to provide advice, counsel, and recommendations for IRB consideration and help to ensure proper management of each investment. The board's mission is to review and evaluate the performance and results of IT investments against projected cost, schedule, performance, and expected mission benefits. All members must be DOL federal employees and authorized to speak on behalf of their parent agencies. As at the IRB, while investments are discussed by PRB, actual funding approval is handled via annual IT Spend Plans and the ITARB.

The charter identifies the Director of IT Budget and Finance Management as the Chair; however, this position does not exist on the High-Level OCIO Organizational Chart (see Figure 2). Other members identified in the charter include the Deputy Chief Information Officer⁹, Director of Enterprise Management Office, Business Product Owner(s), IT Service Owner(s), IT Program Manager/Investment Owner, and Subject Matter Expert(s). The PRB's charter does not identify the specific agencies that are required to attend. This board is to meet bi-monthly and provides oversight over the full lifecycle of IT investments, projects, and services to ensure they are within scope, budget, and timeline. This board is also responsible for reviewing the Service Level Agreement (SLA) performance to negotiate future SLAs with agencies.

⁷ The charter does not specify which of two deputies serves on this board.

⁸ This position does not exist in the High-Level OCIO Organizational Chart (see Figure 2).

⁹ The charter does not specify which of two deputies should serve on the PRB.

ANNUAL IT FUNDING APPROVAL PROCESS

As previously mentioned, the CIO approves IT spending at DOL through one of two methods: 1) annual agency-level IT Spend Plans; or 2) agency submitted IT acquisition requests via the ITARB. Each fiscal year, the CIO works with each agency to develop and approve an agency specific IT Spend Plan. After approval of the IT Spend Plans, any new IT expenses identified that exceed the simplified acquisition threshold require review and approval by the ITARB, which is chaired by the CIO. The ITARB consists of a virtual board with no set meeting frequency nor minutes kept. ITARB requests are received and processed electronically and are recorded in a SharePoint website for tracking purposes.

IT Spend Plans and the ITARB are processes that pre-date the IT Governance Boards. These processes provide the CIO a means to review and approve IT expenses; however, the ITARB is not a formal part of DOL's IT governance structure. Furthermore, while DOL IT governance boards (specifically the IRB) address projects and investments, there is no direct linkage between the ITARB and any DOL-defined IT governance board in DOL's IT spending, outside of the CIO having a role in both institutions.

RESULTS

DOL did not implement an IT governance structure that appropriately aligns authority and responsibility to support the overall mission of the Department. The IT governance structure at DOL remains incomplete and ad hoc, reliant on personnel and limited CIO authority to execute IT strategies. Without a codified IT governance process and an independent role for the CIO in implementing DOL's enterprise-wide IT strategies, the Department's IT assets may be misappropriated, misaligned, or unavailable when needed to support DOL and agency missions.

We found DOL's organizational structure limited the CIO's ability to execute IT governance, resulted in infrequent contact with the most senior level leadership, and left the ASAM to represent IT issues and concerns for several DOL governing boards instead of the CIO. Absent the CIO's ability and authority to execute IT governance oversight, the IT assets of the Department are at risk of not being designed and funded to meet DOL and agency missions.

Recent efforts to centralize IT at the Department successfully shifted control of the majority of agencies' IT operations to OASAM's OCIO. However, two critical agencies, BLS and OCFO, remain largely outside the CIO's purview. We identified that while BLS and OCFO are members of the IT governance boards,

the CIO had limited visibility and control over BLS and OCFO IT systems, IT contract procurements, project management, and IT hardware asset inventory. An inconsistent level of direct access across all agencies hinders the CIO's ability to ensure the safety and availability of all Departmental IT assets.

Across the key elements of IT governance, including DOL's IT Governance model itself, the OCIO had not codified the vital policies and procedures that guide personnel performing their tasks and aide the agencies reliant upon OCIO for IT support. In an ad hoc system where the processes are only as good as the staff currently executing them, the risk for failure through intentional or unintentional efforts remain high.

ALIGNMENT OF CIO LIMITS ENTERPRISE LEVEL VISIBILITY AND AUTHORITY

The organizational alignment of the CIO under the ASAM affected the CIO's ability to execute IT governance at DOL. While our testing found the CIO had approved the sampled IT spending requests, the CIO's reporting relationship limited the CIO's interaction with DOL's most senior organizational leadership independent of the ASAM to whom the CIO reports. This organizational alignment affected the CIO's ability to implement IT changes from a strategic perspective with the CIO absent from leadership of several DOL enterprise boards. Finally, as the CIO reports to the ASAM and provides services to OASAM as a whole, there exists an appearance of and the potential for a conflict of interest that we determined had impacted the CIO's relationship with other agencies served by the OCIO.

Clinger-Cohen Act of 1996 (CCA) was the first time in law that Chief Information Officers were established in government agencies, along with listing their roles and responsibilities. Since the CCA, other key legislation has further defined the role and the relationship of the CIO within a federal organization and what authorities the CIO must hold, most notably: 1) the 2014 Federal Information Technology Acquisition Reform Act (FITARA), and 2) Executive Order 13833 on Enhancing the Effectiveness of Agency Chief Information Officers.

FITARA directed the following concerning IT spending and the CIO role:

(A) IN GENERAL.—The head of each covered agency other than the Department of Defense shall ensure that the Chief Information Officer of the agency has a significant role in—(i) the decision processes for all annual and multiyear planning, programming,

budgeting, and execution decisions, related reporting requirements, and reports related to information technology.

CIO INVOLVED WITH APPROVING IT SPENDING

At DOL, all significant IT purchases must be approved by the CIO in one of two processes, through the submission of IT Spend Plans or through a request to the ITARB.

IT Spend Plans depict an agency's estimated annual IT spending. After IT Spend Plans are approved by the CIO, any IT requests over the simplified acquisition threshold¹⁰ that subsequently arise must be submitted to the ITARB for review and approval. Purchases not included in an agency's IT Spend Plan and which do not exceed the simplified acquisition threshold are not required to be reviewed or approved by the CIO.

We identified 23 ITARB requests processed during fiscal year (FY) 2020. Our analysis determined that all 23 requests had the appropriate approvals and the process was consistent for all DOL agencies, occurring regardless of funding source. Though we remain concerned regarding the CIO's independent visibility and authority over IT spending due to reporting alignment, we determined the process is designed such that the CIO had a role in approving IT spending across DOL and its agencies, consistent with the requirements of FITARA.

CIO REPORTING STRUCTURE

Legislation requiring the CIO to report to the agency head, in DOL's case the Secretary of Labor, originated in the CCA. The Act states:

The head of each agency shall designate a Chief Information Officer who shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter.

FITARA, the first major update to the CCA, left this requirement in place and in 2015, Office Management and Budget (OMB) issued a memorandum, M-15-14, Management and Oversight of Federal Information Technology to provide implementation guidance for the FITARA legislation. Under CIO Role and Responsibilities, the OMB memorandum noted the following:

CIO reports to agency head (or deputy/COO [Chief Operating Officer]). As required by the Clinger Cohen Act and left in place by

¹⁰ As of August 2021, the simplified acquisition threshold was \$250,000.

FITARA, the CIO “shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter.”

This provision remains unchanged, though certain agencies have since implemented legislation under which the CIO and other management officials report to a COO, Undersecretary for Management, Assistant Secretary for Administration, or similar management executive; in these cases, to remain consistent with the Clinger Cohen requirement as left unchanged by FITARA, the CIO shall have direct access to the agency head (i.e., the Secretary, or Deputy Secretary serving on the Secretary’s behalf) regarding programs that include information technology.

More recently, in 2018, Executive Order 13833, Enhancing the Effectiveness of Agency Chief Information Officers was signed, stating the following in regard to the CIO position within an organization:

... the CIO of the covered agency reports directly to the agency head, such that the CIO has direct access to the agency head¹¹ regarding all programs that include IT...

This direct reporting relationship between the CIO and Department leadership, either the Secretary or Deputy Secretary, is essential and should be independent to ensure that the IT priorities for the Department are heard. Any agency voices that can influence or affect the message of the CIO when discussions occur risks jeopardizing the enterprise decisions made and the security of DOL’s information and IT assets. Executive Order 13833 clarified the expected position and relationship of the CIO to the agency head.

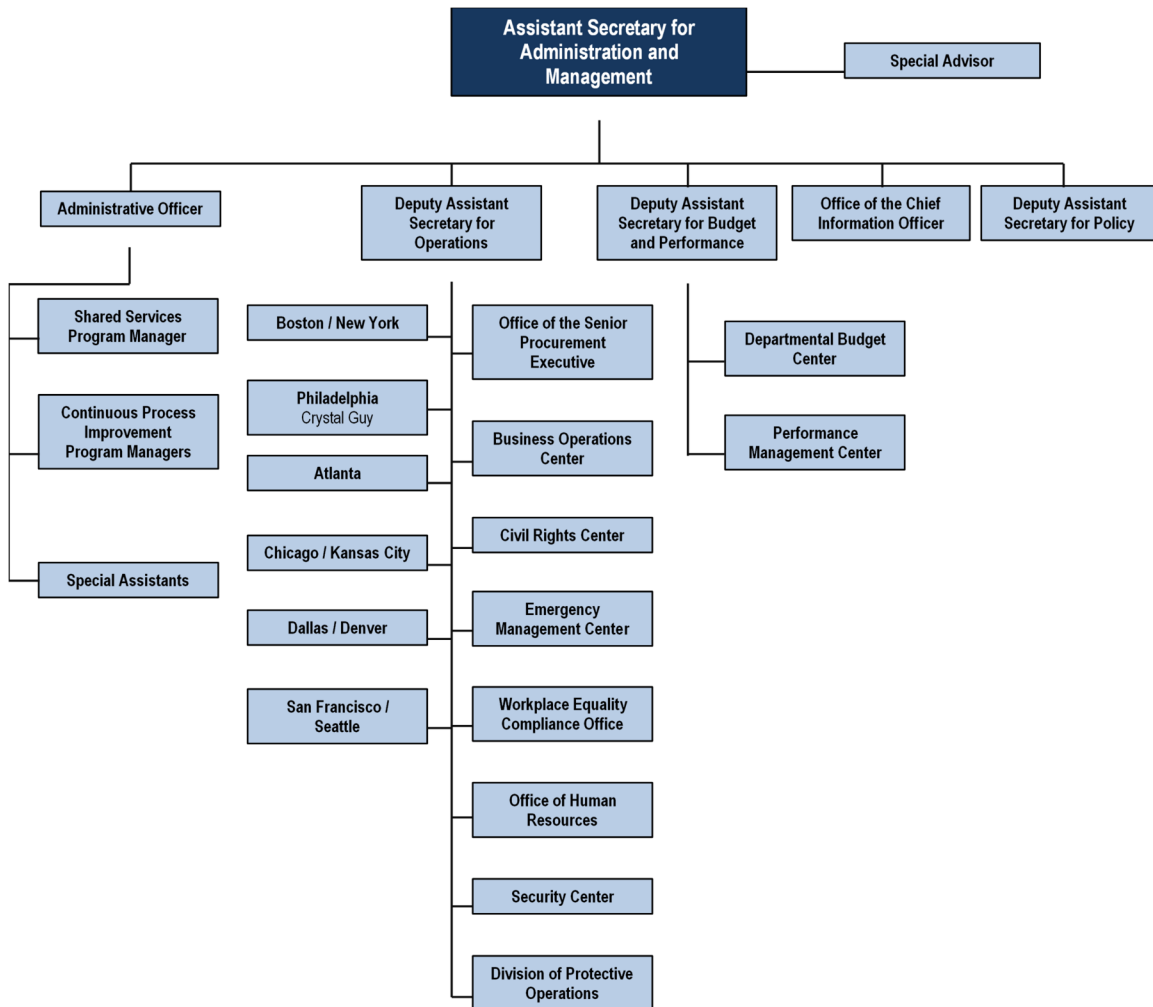
CIO LACKS DIRECT ACCESS TO AGENCY LEADERSHIP

The CIO does not have a direct reporting relationship with the Secretary or Deputy Secretary as mandated by current law or Executive Branch guidance. There is also a lack of independence as the CIO reports to the ASAM, a non-career Senior Executive Service level position and the head of one of the largest customers of the CIO. The ASAM is the CIO’s direct supervisor and conducts the performance evaluation of the CIO. The CIO’s position description states that the CIO receives direction and guidance from the ASAM. Consistent with this description, the OASAM Organizational Chart (see Figure 3) depicts the CIO under the ASAM and on the same level within the OASAM leadership hierarchy

¹¹ Agency head for DOL would be the Secretary of Labor as defined through reference in the Executive Order 13833.

as the Administrative Officer and three Deputy Assistant Secretaries. In addition, the organization chart shows that the OCIO is just 1 of the 23 programs and offices the ASAM is responsible for managing and leading.

Figure 3: OASAM Organizational Chart



Source: DOL Public Webpage

The CIO and prior Deputy Secretary asserted that there is a red line on the Department's overall organizational chart (see Figure 1) connecting the CIO to the Deputy Secretary, with a notation about it indicating direct access. However, the OASAM Organizational Chart (see Figure 3) above does not include notation of this additional access.

Furthermore, the OASAM webpage noted that the CIO and another OASAM executive have a “dotted line reporting relationship” to the Secretary of Labor¹². However, we identified that the DOL organizational chart (see Figure 1) only noted a relationship of this type between the CIO and Deputy Secretary and no relationship for the other executive. This inconsistent approach in documenting a critical line of purported direct access brought into question whether such access existed as described.

We remain concerned that DOL’s reporting alignment and structure for the CIO does not comply with applicable federal requirements. As such we consulted with OIG legal counsel, who provided the following in their legal opinion on the matter:

Addressing the PRA’s [Paperwork Reduction Act] and the CCA’s reporting requirement, Executive Order 13833 (2018) expressly states that the agency CIO is to “report directly to the agency head.” Here we have two relevant authorities, one issued by the legislative branch and one by the executive branch. The two share key language and are [consistent]. In the absence of a judicial ruling that the Order lacks support by statute or the Constitution, the plain language in the Executive Order stands.

DOL’s current positioning of the CIO and DOL’s IT governance structure are not consistent with the plain language of the law as reflected in two statutes and an Executive Order. Additionally, the Department has not provided adequate support to back up its contention that DOL is in compliance with the implementing guidance in OMB-15-14. A single red line on an org chart is not, by itself, evidence of compliance with a reporting requirement between two federal officials.

INDEPENDENCE OF CIO FROM ASAM IN EXECUTIVE COMMUNICATION

To determine the level of independence the CIO maintains from the ASAM in discussions with Department Executives (Secretary or Deputy Secretary), we analyzed meeting attendance from October 2019 to October 2020 involving the CIO, ASAM and DOL Executive Leadership. Our results of this analysis did not support the Department’s assertion that an independent line of communication existed. For example, the ASAM had a standing meeting twice a week with the Deputy Secretary. The CIO may attend these meetings but does not have standing meetings independent of the ASAM. We examined attendance at these

¹² As of our review on September 2, 2021, of OASAM’s organizational chart, this statement has been removed from the webpage.

meetings from October 2019 to October 2020, and found that the CIO was only in 8 of 130 meetings without the ASAM. Whereas, the other 122 meetings involved the ASAM, of whom the CIO is a direct report.

We determined this reflects the substantial difference in the access and interactions of an independent direct report to the Secretary or Deputy Secretary, such as the ASAM, and those of the CIO as an indirect report. Our analysis highlighted the CIO's limited independent communication with the Deputy Secretary and lack of CIO authority at the enterprise level. The Associate Deputy Secretary's response stated that currently the CIO participates in regular weekly meetings with the Deputy Secretary. However, we remain concerned that DOL's organizational alignment of the CIO remains out of compliance with federal requirements.

BENCHMARKING ANALYSIS

We interviewed CIOs at other federal organizations (the National Aeronautics and Space Administration, Department of Interior, Department of Education, Department of Justice, Department of Health and Human Services, and Department of Energy) to identify how their respective agencies approached the positioning of the CIO and the implementation of IT governance. We used these discussions to establish benchmarks in several areas such as reporting, leadership, and strategic involvement. Based on these discussions, we found that five of the six CIOs stated that their position directly reported to the Secretary or Deputy Secretary. Again, and by contrast, the DOL CIO reports to the ASAM and does not have direct access to the Secretary or Deputy Secretary.

Further, four CIOs stated that leadership support of the CIO was important to an effective IT organization, whereas DOL's CIO relied primarily on the ASAM's support. Another key takeaway from our discussion with other federal CIOs was the value of a career official in that position to ensure projects were not impacted by changes in administration, a point also raised by DOL's own CIO when we discussed potential changes to the reporting structure. Additionally, our analysis of the July 2021 FITARA scorecard, a metric of federal agency compliance with FITARA requirements, shows that, of the 24 reporting agencies, DOL remained 1 of only 3 agencies in which the CIO did not report directly to the Secretary or Deputy Secretary¹³. Recent improvements in component FITARA scores by DOL are limited by the scoring penalty DOL incurs due to not having the CIO report directly to the Secretary or Deputy Secretary.

¹³ The other two agencies identified on the FITARA scorecard as not having the CIO report to the Secretary or the Deputy Secretary are Department of Justice and the Nuclear Regulatory Commission.

LIMITED STRATEGIC INVOLVEMENT AT ENTERPRISE LEVEL

At DOL, there are a variety of executive level boards, covering areas and functions such as Management Review, Enterprise Shared Services governance, COVID-19 Response and Enterprise Risk Management. These boards serve to respond to ongoing events, plan for future needs, and execute the strategies of the Secretary. However, the CIO's role is limited in all of these critical enterprise boards.

The Management Review Board (MRB), originally established in 2001 and updated in February 2020 by a Secretary's Order (03-2020), serves as a forum for systematically furthering the Secretary's management objectives. The MRB is co-chaired by the ASAM and CFO with members made up of DOL agency leadership¹⁴. Unlike the co-chairs and the DOL agency leadership, the CIO was explicitly identified as a non-member subject matter expert to provide information and guidance to the MRB. Additionally, the CIO is not a member of independent committees, boards, or councils that report information and updates to the MRB. Though the Associate Deputy Secretary's response to our draft of this report noted that we refer to the Management Review Board that is not currently utilized, as of issuance of the draft report in September 2021, the Secretary's Order reestablishing the Management Review Board in March 2020 had not been rescinded.

The Enterprise Shared Services governance board oversees the IT Governance boards including the IRB chaired by the CIO. According to the Secretary's order that established ESS:

Each service-specific board will operate in accordance with a charter, which shall be reviewed with input from DOL client agencies and approved by the ESS governance board and Deputy Secretary. These service-specific governance boards will provide information and reporting to the ESS Governance Board chaired by the ASAM

The ESS Governance Board, chaired by the ASAM, included standing board membership by a representative of the Deputy Secretary's office and three Deputy Assistant Secretaries of OASAM. The CIO supports the ESS in an advisory role but has no permanent or rotating board membership. This reporting structure again furthers concerns about the CIO's ability to execute IT strategy.

¹⁴ Secretary's Order 03-2020 identifies members as DOL Agency Heads or their designee. Designees will be at the Deputy Assistant Secretary level or the Agency's Administrative Office.

In March 2020, DOL moved to a maximum telework posture and named the ASAM as the Department's official for COVID response. In August 2021, the Department updated the COVID Workplace Safety Plan to note the ASAM remained the lead for COVID-19 planning and response. In addition, the Department created a COVID-19 coordination team to advise the Secretary and ASAM. This team is made up of seven members: Secretary of Labor; ASAM, OSHA Deputy Assistant Secretary; OSHA Deputy Director of Standards and Guidance; Chief Human Capital Officer; Director of OASAM BOC and Solicitor of Labor. This critical team for dealing with the ongoing pandemic does not have the CIO as a member.

An area of importance to the Department's overall governance is Enterprise Risk Management (ERM), which is carried out through the Enterprise Risk Management Council (ERMC). The ERMC's mission is to increase transparency, leadership collaboration, reduce costs, and better enable the Department to manage its risks. The OCIO provided enterprise IT risks to the ERMC but did not necessarily consider non-OCIO, agency-specific IT risks. Agencies may consult with OCIO staff to determine IT risks for their agency submission, but are not required to do so, potentially leaving the CIO unaware of agency-specific IT risks and creating a gap in the ERM process. Further, we found the CIO attended the ERMC as a council member, not as part of its leadership and therefore, not in a decision-making capacity. The ERMC was co-chaired by the Deputy Secretary, the CFO, and the ASAM.

During our benchmarking discussion with other federal CIOs, four CIOs stated that the CIO should be a strategic leader with a seat at the table to make decisions, whereas at DOL, the CIO was not a formal member at any of the Executive level boards. Further, the three IT governance boards (IRB, EARB, and PRB) do not have any membership by the Secretary or Deputy Secretary, leaving them without executive-level presence. This lack of CIO input at the executive level could leave Departmental leadership missing critical IT insights or concerns when decisions are made and risks are considered. Our benchmarking confirmed that a career CIO empowered by their leadership has been an effective approach across the federal government.

FITARA notes that with regard to enterprise oversight of IT:

...The head of each covered agency other than the Department of Defense shall ensure that the Chief Information Officer of the agency has a significant role in ... the management, governance, and oversight processes related to information technology.

At DOL, the CIO was not positioned to directly and independently communicate IT perspectives and concerns at the highest levels of organizational leadership

and, therefore, did not have the significant role required by FITARA. Without CIO decision-making authority at the table, DOL leadership could make decisions that overlook IT concerns or do not properly incorporate IT knowledge.

POTENTIAL FOR CONFLICTS OF INTEREST

In 2015, the OIG's Federal Information Security Modernization Act (FISMA) annual review identified the reporting structure of the CIO as a concern and recommended¹⁵ realigning the organizational structure to address the CIO's independence. Since that time and under the ASAM's Enterprise Shared Services initiative, the role of the DOL CIO changed with the transitioning of IT accountability, authority, and operations from the agencies to a central authority within OCIO. This new structure created a true client-customer relationship between OCIO and DOL agencies. However, given DOL's current organizational structure, the OCIO still existed within one of its largest customers, OASAM, and under the control and supervision of the ASAM.

During interviews with DOL agency leadership in 2020, concerns were raised regarding this relationship between OASAM and OCIO, which some felt could lead to preferential treatment in either direction. For example, there could be prioritized human resource activity for OCIO by OASAM or special IT considerations for OASAM by OCIO. In addition, one agency leader noted they preferred the current structure because if the CIO did not agree with the agency leader, this agency leader could go over the CIO to the ASAM because the ASAM is the agency lead's peer. In fact, agencies signed their IT Shared Services MOUs with the ASAM, not the CIO, even though the OCIO is responsible for providing the IT services.

DOL's organizational structure does not clearly indicate the authority and responsibility expected of the CIO position and mandated by law through its reporting alignment. In interviews conducted, neither the former Deputy Secretary nor the former ASAM could provide a reason for not realigning the OCIO. The consensus was an "if it's not broke, don't fix it" mentality. The former ASAM could provide nothing to evidence that moving the CIO would be detrimental to mission success. In fact, the former ASAM noted, "[w]e help OCIO get done the things they need to get done." This implied that the OCIO could not get things done without OASAM's help and, therefore, if OASAM did not support a CIO initiative, then the former ASAM could effectively halt it given their organizational relationship, impairing the CIO authority and effectiveness as a strategic leader. In its current state, the positioning of the CIO within OASAM at

¹⁵ FISMA 2015 report issued September 2016, for details see <https://www.oig.dol.gov/public/reports/oa/2016/23-16-002-07-725P.pdf>

DOL and the limited relationship to senior leadership subjects the organization to potential conflicts of interest.

Without the support of leadership at the highest levels through an independent direct relationship with the Deputy Secretary, the CIO remains dependent upon the support of the ASAM to ensure CIO priorities are raised with the Deputy Secretary. Conversely, efforts of the CIO that the ASAM opposes may not receive the support necessary. Finally, the recent changes brought by IT Shared Services left the CIO open to the appearance of preferential treatment by or for OASAM, which could disrupt OCIO working relationships with other agency partners. Any one of these situations could lead to the weakening of IT governance at the Department, leaving critical infrastructure, or mission-sensitive information vulnerable in the process. Our benchmarking confirmed that a career CIO empowered by their leadership has been an effective approach across the federal government.

BLIND SPOTS EXISTED IN IT GOVERNANCE ACROSS DOL AGENCIES

As of January 2021, BLS and OCFO remained independent of the OCIO's IT Shared Services initiative, leaving the CIO without adequate visibility and authority over DOL IT in a number of critical areas.

Of the 70 FISMA reportable systems¹⁶ at DOL, the CIO was identified as the Authorizing Official for 49 systems. Of the 21 remaining systems, 13 were not incorporated into IT Shared Services, including all BLS and OCFO systems.¹⁷ There is a substantial difference in visibility and control over systems where the CIO serves as the Authorizing Official versus those of BLS and OCFO where the CIO remains reliant upon the agency. As long as gaps in the CIO's visibility and authority across DOL agencies exist, the Department will remain in a vulnerable IT posture.

Through the Department's Enterprise Shared Services initiative, DOL was working to avoid duplication of resources and ensure cost savings, as appropriate, across the DOL enterprise. However, to achieve this goal for IT

¹⁶ A FISMA-reportable system is an information system that supports the operations and assets of the agency, and FISMA requires the agency to implement an agency-wide program for information security for those systems.

¹⁷ Other exceptions include the Office of the Solicitor (SOL) Evidence Management System (EMS); five OIG systems due to independence concerns; and two Job Corps system, pending Job Corps' incorporation into IT Shared Services.

resources, the CIO must have visibility over all IT investments, including IT procurement, the lifecycle of IT projects, and the inventory of IT assets.

The Secretary's Order 07-2020, dated June 22, 2020, which established Enterprise Shared Services, noted that:

The purpose of ESS is to minimize the duplication of resources within the Department and to establish a centralized administrative services system that is consistent, efficient, and measurable, thereby enabling agency staff to devote more time and resources to the Department.

In addition, the OMB memorandum Chief Information Officer Authorities (M-11-29) stated "CIOs must drive the investment review process for IT investments and have responsibility over the entire IT portfolio for an Agency."

LIMITED VISIBILITY AND CONTROL OVER IT PROCUREMENTS, PROJECT MANAGEMENT, AND ASSET INVENTORY

For all agencies, excluding BLS and OCFO,¹⁸ we found OCIO was involved with all aspects of agency IT procurements. Agencies work with OCIO and OASAM's Office of the Senior Procurement Executive (OSPE) to fulfill these procurement actions, with OCIO maintaining access to the respective contracts. However, for BLS and OCFO, the respective agency controlled and maintained the contracts, and OCIO can only access the contracts by requesting them from OCFO or BLS as needed.¹⁹ The 199 contracts held by BLS and OCFO encompass over 30 percent of DOL's combined IT contracts (637 contracts in total) and amount to nearly \$243 million in value. This staggering amount of IT spending and related contract oversight remained outside of OCIO visibility and control. Without the ability to manage DOL's complete IT procurement portfolio, the CIO may be unaware of key contract clauses, modifications, or updates that could affect the security of DOL data and systems. Further, the CIO was not positioned to best manage the efficiency of DOL resources spent under these contracts. In addition, with the placement of OCIO and OSPE both within OASAM, the ASAM maintains final say over any disagreements regarding IT contract procurements.

According to OCIO leadership at the time of our review, IT projects at DOL for all agencies, excluding BLS and OCFO, were managed by project managers in the appropriate OCIO branch/division/directorate (e.g., Business Application

¹⁸ The OIG is excluded as well due to independence requirements.

¹⁹ For MSHA MEO, OCIO does not handle its IT procurement and does not have access to its contracts.

Services) in consultation with business leads at the agency. The IT project managers utilized a common project management software that the Division of Enterprise Program Management maintains. IT project management for BLS and OCFO were handled internally using their own project management software. Since OCIO does not have access to this software to review information directly, OCIO relied upon informational extracts from BLS and OCFO, respectively, and remained a limited participant in the ongoing management of IT projects at these agencies.

Asset inventory for BLS also remained an area of limited visibility for OCIO. OCIO leadership informed us that the OCIO managed the Department's accountable IT hardware assets, to include assignment and location information for all Department agencies, excluding BLS and Job Corps.²⁰ While Job Corps was in the process of shifting to IT Shared Services at the time of our testing, BLS has its own IT hardware asset tracking system that OCIO does not have access to and must rely on BLS for data extracts limiting OCIO visibility over the assets without BLS intervention. This CIO blind spot is particularly concerning, given prior OIG reporting of IT inventory concerns, including missing assets.²¹

As of June 2020, an interview with the BLS Commissioner indicated they were negotiating with OCIO to determine what portion of its IT systems and asset inventory would transition under OCIO control through IT Shared Services. In November 2020, the OIG was informed that the Deputy Secretary, after our interview with the BLS Commissioner, had decided to pause BLS and OCFO integration into IT Shared Services. For OCFO, the Deputy Secretary did not want to move them during an ongoing audit. With regard to BLS, the Deputy Secretary thought such a move was not prudent at the time, given the potential that BLS may transition over to the Department of Commerce. The CIO indicated both decisions would be reviewed in 2021, and that he saw value in fully incorporating both BLS and OCFO into IT Shared Services.²²

The purpose of centralizing IT was to ensure the CIO was best positioned to oversee procurement and utilization of enterprise-wide IT resources and has proper visibility to make decisions on behalf of the Department. With the substantial IT posture of BLS and OCFO, the delay in fully integrating these

²⁰ OIG was not tracked by OCIO; MSHA MEO was tracked in ServiceNow but managed by MSHA personnel following OCIO procedures.

²¹ Department of Labor. 2021. *Semiannual Report to Congress (October 1, 2020 – March 31, 2021): Volume 85*. Washington, DC: Department of Labor.
<https://www.oig.dol.gov/public/semiannuals/85.pdf>.

²² As of July 2021 DOL Leadership has not made a determination for incorporating either agency fully into IT Shared Services.

agencies into IT Shared Services prolonged the CIO's inability to fulfill the requirements of legislation and ensure enterprise security and architectural alignment of IT resources.

**KEY IT GOVERNANCE ELEMENTS
REMAINED AMBIGUOUS DUE TO AD HOC
EXECUTION**

DOL's IT governance model, as well as other critical governing elements, remained undefined and left the Department reliant on personnel to execute ad hoc processes in lieu of established, documented policies and procedures. Additionally, with the recent transition to IT Shared Services, the absence of clearly documented requirements and processes created confusion among agencies dependent upon OCIO for IT support.

Between fiscal year 2018 and fiscal year end 2020, the implementation of IT Shared Services resulted in the expansion of OCIO staff from 125 federal employees to 341 federal employees. Additionally, contractor staff within the OCIO increased dramatically from 588 to 1,310 over the same period. This substantial growth in a short amount of time meant considerable new responsibilities for existing OCIO personnel and necessitated integrating numerous new OCIO personnel into existing processes. However, we found that policies and procedures were not developed, codified, or implemented prior to or in conjunction with the development of the new OCIO organizational makeup and the re-assignment of agency staff to the OCIO.

We identified four key components of IT governance - contract procurement, project management, client engagement, and asset inventory – and sought to determine the extent to which enterprise-wide processes were established and codified for managing in each of these critical areas. For these key areas, we identified that procedures in place were not documented and relied heavily on the institutional knowledge of personnel in place to ensure they were performed in line with CIO expectations. This ad hoc procedural environment could be difficult for new personnel to understand and put client agencies at risk of service interruption if personnel involved changed. In addition, for the client agencies attempting to learn what services OCIO can provide or how to best address an issue, the lack of codified information and clear lines of communication created ambiguity and increased operational risk.²³

²³ At the time of work, none of the key areas we examined had codified policies or procedures, nor were there draft procedures in development.

In 2018, the ASAM contracted with Booz Allen Hamilton Holding Corporation to perform a review of the OCIO organizational structure. The results of this review, which were presented to the Deputy Secretary, suggested a new organizational structure does not operate in a vacuum, and should be supported by several critical components. The components identified consisted of clearly defined roles and responsibilities, documentation on how decisions are made, and identification of communication channels across OCIO and between OCIO and its client agencies. The report further stated these components are critical to organizational success and should be developed in detail early on in the new organization's maturation.

Although the CIO developed a Functional Organizational Design document that contained detailed definitions and descriptions for the new directorates and their underlying divisions, the document was never published or utilized. According to OCIO management, the Functional Organizational Design document had not been distributed to staff and is subsequently being revised to align with how these groups were functioning at the time, in lieu of the document driving the development of these functional areas, as originally intended.

AMBIGUITY IN DOL'S IT GOVERNANCE MODEL

According to the CIO, DOL's IT Governance Model at the time of our work consisted of the charters for the three key governance boards: IRB, EARB, and PRB. The CIO stated that the charters for each board represented the governance framework; however, these charters do not create any linkage between the boards. Further, this governance model does not support a clear, collaborative process providing transparency to agencies on how IT initiatives are proposed, reviewed, approved, and managed. Finally, the model does not provide a mechanism that allows agencies to provide input on the IT governance process and receive feedback on how it is working.

DOL's IT governance model does not cover the depth and breadth of roles and functions involved in governing DOL's IT assets, including how the boards interact with agencies, each other, and other elements such as the IT security function. In addition, the relationship of IT spending and IT procurement to these IT governance boards remains undefined. Outside of the charters, the Department had not clearly defined, communicated, or codified its IT governance and new OCIO structure.

Efforts to make the changes required by IT Shared Services, such as transitioning personnel and responsibilities into OCIO, were effectuated quickly, and did not pause for the development and codification of processes for how the new functions would work. According to the CIO, the OCIO is focused on

remedying the lack of codified documentation of the various inputs and workings around the boards in a full IT governance model.

MEMORANDUMS OF UNDERSTANDING

DOL agencies incorporated as part of IT Shared Services initiative signed MOUs between agency leadership and the ASAM to define roles and service level requirements; however, we found not all agencies or programs were utilizing these MOUs for IT services. We identified that OASAM's Business Operations Center, Office of Human Resources, and Departmental Budget Center were excluded from these agreements on IT services. Additionally, agencies that did not transfer personnel to the OCIO in support of the IT Shared Services initiative, or previously relied upon the OCIO for their IT support, did not have MOUs established.

Finally, these MOUs defining IT roles and service level responsibilities were all signed by the ASAM not the CIO indicating the authority and responsibilities lie with the ASAM.

As such, we found that although BLS and OCFO are responsible for nearly a third of the Department's IT contracts procured, neither had MOUs in place with OASAM or OCIO to document the IT roles and responsibilities of the respective agencies.²⁴ Without defined roles and responsibilities of OCIO, and the services to be provided to an agency, IT assets could be at risk.

CLIENT ENGAGEMENT

Communication is a critical component of any successful organization, and clear, well-defined lines of communication are key to ensuring consistency of message. The Client Engagement Division maintains this role within OCIO. According to the OCIO's Functional Organizational Design document, the Client Engagement Division within OCIO is responsible for understanding the functional and technical issues that clients face and communicating these issues to the appropriate parties within OCIO. This group has several potential points of contact such as the joint business planning meetings, the demand review meetings, and meetings with agencies, but the procedures, both internal and agency-specific, are not codified. Additionally, they allow the agencies to determine whom they want the client engagement managers to engage with, which adds another layer of inconsistency to a process that is not clearly defined or communicated to stakeholders. Ultimately, we found the focus on executing a

²⁴ The OIG also did not have an MOU in place with OASAM or OCIO for this purpose.

new process of client engagement for multiple agencies in a short timeframe led to undefined procedures governing how to maintain client engagement.

The lack of process codification was also clearly on display within the areas of IT procurement, project management, and asset inventory. Our discussions with OCIO management within these areas revealed that none of them had clearly defined procedures that would help ensure they operated consistently and understood the key points of communication between directorates and client agencies that would support operational efficiency and effectiveness for their areas of responsibility. All three of these key areas were impacted by the focus on integrating personnel from multiple agencies and the rush to set up these key areas adversely affected the development of much needed procedures.

For example, based on interviews with OCIO procurement and OSPE, there were no documented procedures specific to how the IT contracting process should function between their two groups. Instead, they relied on processes that were in place prior to the IT Shared Services initiative with stopgap measures such as email and staff knowledge to ensure that IT contracts were processed correctly and that no IT procurements were missed. Further, the OCIO IT Procurement Branch made it clear that while the responsibilities were transferred, they were still in the process of absorbing new staff and trying to get a handle on all the IT contracts for the agencies that recently transitioned to the IT Shared Services model. To maintain IT security, OCIO stated it was aware they needed to re-organize and document internal processes.

Codification and documentation of policies and procedures are critical to ensure personnel know what to do and agencies know where to turn for vital information. federal law on Records Management by federal agencies (44 U.S.C. Chapter 31) states:

The head of each federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and [be] designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

In addition, OMB Circular A-123 - Management's Responsibility for Internal Control states:

Generally, identifying and implementing the specific procedures necessary to ensure effective internal control, and determining how to assess the effectiveness of those controls, is left to the discretion

of the agency head. While the procedures may vary from agency to agency, management should have a clear, organized strategy with well-defined documentation processes that contain an audit trail, verifiable results, and specify document retention periods so that someone not connected with the procedures can understand the assessment process.

The importance of clearly defining and communicating the objectives, key responsibilities, and outputs of the new directorates, and description of the key interfaces, collaboration, and integration points with other directorates as well as the client agencies, cannot be understated. When the policies and procedures at the Department rely entirely upon the people who perform the tasks with no codified record, then there is always the risk that at any moment, these ad hoc procedures could be changed or lost, intentionally or not, simply with the loss or re-assignment of a key staff member. In cases where the current procedures are effective, the assurance of future viability is lost if they remain ad hoc. In addition, without documented procedures to follow, accountability is lost for the client agencies, who rely on OCIO to perform a variety of services. Further, for OCIO personnel themselves, the accountability of staff to perform their jobs is difficult to meet when nothing is reliably documented. Finally, with no codified policies in place across key IT governance areas, there is increased risk that IT governance functions are not understood across the Department.

CONCLUSION

With limits on CIO authority, both by structural design and by lack of representation at enterprise level discussions, the CIO was not fully empowered to ensure IT governance at DOL was effectively implemented. Discussions with other federal agencies confirmed that a career CIO with the backing of senior leadership was the most effective structure for organizational continuity. Given the recent, significant changes in DOL's IT service model, DOL needs to reevaluate its organizational leadership structure and elevate the CIO position to ensure it is postured to interact and provide independent leadership during enterprise strategic planning and decision meetings.

Furthermore, while DOL has been implementing the IT Shared Services approach for over two years, documentation of roles, responsibilities, and processes for governing and providing IT services were not developed and documented. With most DOL agencies now transitioned under the IT Shared Services model, the OCIO will need to focus on reviewing and codifying its processes.

We acknowledge recent successes accomplished in executing the Enterprise Shared Services initiative. The Department recently transitioned successfully to maximum telework under the former ASAM's leadership for COVID-19 response at the Department. However, the current COVID-19 coordination team responding to the continued challenges of the pandemic does not include the CIO as a member. Additionally, with the lack of documentation and codified processes future positive outcomes are not assured as personnel may change and execute functions differently.

OIG'S RECOMMENDATIONS

To improve DOL's establishment and implementation of IT governance across the enterprise, we recommend the Deputy Secretary:

1. Reorganize the CIO position to have a direct reporting relationship to the Deputy Secretary and independent of ASAM.
2. Ensure the CIO is a lead member with voting rights of DOL's executive strategy and management boards and committees including but not limited to the MRB, ESS Governance Board, COVID-19 Coordination team, and ERMIC.
3. Reassess the incorporation of BLS and OCFO as part of IT Shared Services within 2021, and document the reasoning for the decision reached.
4. Establish an MOU or other agreement between the OCIO and all departmental agencies to establish and state the roles and responsibilities of IT between each set of respective agencies.
5. Codify the policies and procedures that define IT governance and key supporting IT elements.

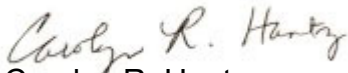
SUMMARY OF THE DEPARTMENT'S RESPONSE

The Associate Deputy Secretary for the Department disagreed with one recommendation to provide the CIO with the authority, accountability, and independence required to effectively manage the Department's IT by elevating the CIO to level commensurate with DOL's Assistant Secretaries and the CFO in

reporting to the Deputy Secretary. The Associate Deputy Secretary accepted the other four recommendations and will develop a plan to implement them.

The Associate Deputy Secretary's full response can be found in Appendix B.

We appreciate the cooperation and courtesies OASAM, OCIO, and other DOL officials extended us during this audit. OIG personnel who made major contributions to this report are listed in Appendix C.



Carolyn R. Hantz
Assistant Inspector General for Audit

**EXHIBIT 1: CUSTOMER AGENCIES OF OCIO PRIOR TO IT
SHARED SERVICES**

The following five agencies were reliant upon OCIO for their IT support prior to IT Shared Services initiative:

1. Office of Congressional and Intergovernmental Affairs (OCIA)
2. Office of Disability Employment Policy (ODEP)
3. Office of the Assistant Secretary for Policy (OASP)
4. Bureau of International Labor Affairs (ILAB)
5. Ombudsman for the Energy Employees Occupational Illness Compensation Program (EEOMBD)

EXHIBIT 2: CUSTOMER AGENCIES OF OCIO UNDER IT SHARED SERVICES

These 18 agencies moved into IT Shared Services as of January 2021:

1. Administrative Review Board
2. Benefits Review Board
3. Employee Benefits Security Administration (EBSA)
4. Employee's Compensation Appeals Board
5. Employment and Training Administration (ETA)
6. Mine Safety and Health Administration (MSHA)
7. Occupational Safety and Health Administration (OSHA)
8. Office of Administrative Law Judges (OALJ)
9. Office of Federal Contract Compliance Programs (OFCCP)
10. Office of Labor-Management Standards (OLMS)
11. Office of Public Affairs (OPA)
12. Office of the Assistant Secretary for Administration and Management (OASAM)
13. Office of the Secretary (OSEC)
14. Office of the Solicitor (SOL)
15. Office of Worker's Compensation Program (OWCP)
16. Veterans Employment and Training Service (VETS)
17. Wage and Hour Division (WHD)
18. Women's Bureau (WB)

APPENDIX A: SCOPE, METHODOLOGY, & CRITERIA

SCOPE

Our audit covered DOL's IT governance framework and implementation from January 2020 through March 2021. Our review of the Department's governance framework included close analysis of key IT services such as IT spending, procurement, operations, and Enterprise Risk Management.

METHODOLOGY

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To answer our audit objective, we conducted interviews with officials within OCIO as to the current state of IT governance. We evaluated documentation related to IT governance, conducted benchmarking activities of DOL's IT governance structure with that of other federal agencies, and created surveys to gain DOL agency perspectives as to the impact of IT governance on their agencies. We interviewed the Deputy Secretary, ASAM, and other officials throughout DOL, as well as select employees of DOL's OCIO, including the CIO. In addition, we interviewed the CIOs, OCIO representatives, and OIG representatives of the National Aeronautics and Space Administration, Department of Interior, Department of Education, Department of Justice, Department of Health and Human Services, and Department of Energy. This report represents the culmination of our efforts in this endeavor.

We performed our fieldwork at DOL headquarters in Washington, DC beginning in January 2020. We transitioned to continue our fieldwork remotely due to the COVID-19 pandemic in February 2020. Management was informed of the changes in work. There was no impact to the quality of work performed on this audit due to completing the audit in a remote environment.

We did not solely rely on any OCIO data to support findings, conclusions, or recommendations. As such, we did not perform a specific assessment of the reliability of computer-processed data.

In planning our audit, we identified the internal control standards relevant to our performance audit of DOL IT governance. These included internal control audit standards primarily found in the Government Accountability Office (GAO) Yellow Book and the DOL Office of Audit Handbook (or Bluebook). In planning and performing our audit, we considered OCIO's internal controls relevant to our audit objective by obtaining an understanding of those controls and assessing control risks for the purpose of achieving our objective. The objective of our audit was not to provide assurance of the internal controls; therefore, we did not express an opinion on OCIO's internal controls.

CRITERIA

- 44 USC Chapter 35, Coordination of Federal Information Policy – Section 3506: Federal Agency Responsibilities
- Executive Order 13833 Enhancing the Effectiveness of Agency Chief Information Officers Issued on May 15, 2018
- OMB Memo M-15-14 FITARA Implementation
- Public Law 104–106—FEB. 10, 1996 also known as The Clinger-Cohen Act of 1996
- Public Law 113–291—DEC. 19, 2014 (Subtitle D—Federal Information Technology Acquisition Reform: Sec 831- Sec 837)

PRIOR COVERAGE

During the last 5 years, we have issued two reports of significant relevance to the subject of this report. Unrestricted reports can be accessed at <https://www.oig.dol.gov/auditreports.htm>, and include the following:

1. FISMA Fiscal Year 2015: Ongoing Security Deficiencies Exist 2015 (Report Number: 23-16-002-07-725P, Issued November 30, 2016)
2. FY 2018 FISMA DOL Information Security Report 2018 (Report Number: 23-19-001-07-725, Issued March 13, 2019)

Additionally, a GAO report relevant to the subject of this report is:

FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities, Issued August 2018, available at <https://www.gao.gov/assets/gao-18-93.pdf>

APPENDIX B: AGENCY'S RESPONSE TO THE REPORT

U.S. Department of Labor

Office of the Deputy Secretary
Washington, D.C. 20210



September 24, 2021

MEMORANDUM FOR Carolyn R. Hantz

Assistant Inspector General for Audit

FROM:

NIKKI MCKINNEY *Nikki McKinney*
Associate Deputy Secretary

SUBJECT:

Draft Report on DOL's IT Governance,
Report Number: 23-21-002-01-001

Thank you for the opportunity to review and respond to the Office of Inspector General's (OIG) September 10 draft audit report concerning the Department's IT governance framework. It is the Department's practice to actively engage with OIG auditors and fully cooperate. As we have said previously during this audit engagement, we recognize OIG's audits can make meaningful contributions to efficiency and effectiveness of the Department's overall mission delivery. The key to adding value is well-informed audits that are fair and balanced, and offer useful, achievable recommendations for the improving DOL program administration. For the reasons outlined below, I find these attributes still lacking in the draft audit report, deficiencies which are amplified by the audit's continued focus on form over substance.

By memorandum of August 20, 2021, the Office of the Deputy Secretary replied to the initial draft audit report on DOL's IT Governance. Except for passing acknowledgement, virtually none of our comments and concerns expressed in our August 20 reply were incorporated in the September 10 draft audit report. Mindful that the readership of OIG audit reports includes the public, DOL stakeholders, and our congressional overseers, I will restate and summarize many of them here as they pertain to the September draft report:

As acknowledged in the draft audit report, the Department undertook a significant realignment of its IT resources, consolidating IT functions into an IT Shared Services model and moving the majority of former agency information technology specialists under the direction of the Department's Chief Information Officer (CIO). This strategic realignment greatly expanded the CIO's scope of authority and the effectiveness in how DOL provides IT services in support of agency missions. To be fair and balanced, the audit report should include this context.

The improved effectiveness and efficiency of the CIO and restructured organization—and implicitly the sufficiency of the CIO's authority—are plain to see:

- The Department swiftly and successfully pivoted to a maximum telework posture for the vast majority of agency staff—more than 99% of DOL staff—in response to government-wide COVID-19 mitigation policies.

- The Department has steadily improved its annual Federal Information Technology Acquisition Reform Act (FITARA) scorecard grades, most recently achieving 6 “A’s” and one “B”. For perspective, DOL was one of just two agencies to receive 6 “A’s” on its July 2021 FITARA scorecard. While this grade held steady from the December 2020 scorecard, it is no easy feat to maintain this level of performance while also integrating DOL agency IT units into the Shared Services model and providing the IT services required by COVID-19 mitigation policies.
- The Department, under the direction of the CIO, has closed 94 IT-related OIG recommendations in the last three years, scored an increase in 35 OIG Federal Information Security Modernization Act (FISMA)-assessed metrics in the last two years, earned an OIG-rated FISMA maturity level greater than 16 of 22 other CFO Act Agencies, and has achieved 10 of 10 President’s Management Agenda Cyber Cross Agency Priority Goals.
- The OCIO has partnered with the Departmental Budget Center to clearly articulate IT strategy and progress to OMB and Congress in support of agency modernization initiative requests resulting in the efficient use of expired funds to invest in IT modernization.
- The OCIO built processes for lateral collaboration with Procurement, Budget, and Human Resources—a central purpose of FITARA.
- The OCIO has implemented a number of communication channels to ensure agencies have two-way communications with their IT support.
- The Department, with its CIO leading the strategy, has initiated numerous IT modernization efforts that include:
 - Cloud modernization
 - Established a private cloud offering for hosting and storage to provide scalable hosting capacity, eliminating storage limitations, and facilitating backup and disaster recovery.
 - Migrated 37 DOL mission applications or services to the cloud to enable scalable computing capacity for seasonal business processes like visa applications.
 - Digital transformation
 - Consolidated DOL.gov web sites to the OCIO Content Management Platform which standardized the format of multiple unique sites, centralized and simplified maintenance requirements, enabled hosting scalability to address peak traffic demands (such as the peak days resulting from coronavirus guidance publishing), and enabled agency personnel to manage their own content.

- Established case management platform for systems like OFLC Foreign Labor Applications Gateway, OSHA Injury Tracking system, or the OFCCP Affirmative Action Verification Initiative by establishing DOL standard components, establishing common development practices, developing reusable add-on capabilities, and standardizing maintenance processes.
- Cybersecurity enhancement
 - Expanded cybersecurity security operations to monitor traffic on a 24/7 basis for threat reduction and to improve incident tracking and reporting.
 - Continued implementation of DHS mandated cybersecurity toolset to ensure DOL meets or exceeds requirements and ultimately minimizes the chances of adverse incidents.
 - Implemented a practice of ongoing authorization instead of “Authority to Operate” authorization engagements every three years for OCIO-managed systems to provide more predictable workloads and minimize the security impact of system changes.

Despite objective evidence of the authoritative role of the Department’s CIO and enhanced organization under the Shared Services model, the draft audit zeros in on process rather than outcomes. The draft audit report opines that the Department’s CIO reporting alignment and structure does not comply with federal requirements, citing among other authorities the Clinger-Cohen Act of 1996, FITARA, and Executive Order 13883 (2018), which in relevant part provides:

Sec. 4. Emphasizing Chief Information Officer Duties and Responsibilities. The head of each covered agency shall take all necessary and appropriate action to ensure that:

- (a) consistent with 44 U.S.C. 3506(a)(2), the CIO of the covered agency reports directly to the agency head, such that the CIO has direct access to the agency head regarding all programs that include IT.

From this foundation, the September draft audit report reasons as follows:

“To determine the level of independence the CIO maintains from the ASAM in discussions with Department Executives (Secretary or Deputy Secretary), we analyzed meeting attendance from October 2019 to October 2020 involving the CIO, ASAM and DOL Executive Leadership. Our results of this analysis did not support the Department’s assertion that an independent line of communication existed. For example, the ASAM had a standing meeting twice a week with the Deputy Secretary. The CIO may attend these meetings but does not have standing meetings independent of the ASAM. We examined attendance at these meetings from October 2019 to October 2020, and found that the CIO was only in eight of 130 meetings without the ASAM. Whereas, the other 122 meetings involved the ASAM, of whom the CIO is a direct report.

We determined this reflects the substantial difference in the access and interactions of an independent direct report to the Secretary or Deputy Secretary, such as the ASAM, and those of the CIO as an indirect report. Our analysis highlighted the CIO's limited independent communication with the Deputy Secretary and lack of CIO authority at the enterprise level. As a result, we determined DOL's organizational alignment of the CIO remains out of compliance with federal requirements."

This analysis suffers from several flaws, the first of which is that Executive Order 13883 does not specify an "independent line of communication" for the CIO. It directs that "...the CIO of the covered agency reports directly to the agency head, *such that the CIO has direct access to the agency head regarding all programs that include IT.*" [Emphasis added]

Second, this analysis rests on the flawed assumption that only meetings of the CIO with the Secretary and/or Deputy Secretary, in the absence of the Assistant Secretary for Administration and Management, constitute "direct access to the agency head". The auditor's analysis documents that the Department's CIO has ample direct access to the agency head, according to the draft audit report averaging over ten meetings a month with the Secretary and/or Deputy Secretary for the period of October 2019 to October 2020.

Perhaps most troubling is a lack of understanding by the auditors of how DOL Executive Leadership functions. One-on-one meetings with the CIO and the agency head do not, in and of themselves, produce results different from those that are achieved in meetings attended by other relevant participants. Goals and outcomes are achieved by marshalling the organization's component parts to achieve success. One might imagine, in the auditor's view, the CIO is both quarterback and receiver, throwing the ball and then catching it. Instead, the Department's career CIO is empowered by DOL leadership, including the ASAM, to implement the vision of the CIO.

To this latter point, I note with interest the passage from the September 10 draft report Conclusion: "Discussions with other federal agencies confirm that a career CIO with the backing of senior leadership was the most effective structure for organizational continuity" This is the model at DOL and, for a Department of this size and configuration, it works very well.

Additionally, the report needs to be explicitly clear that this audit was conducted before the current Department's leadership implemented its practices. For example, the report refers to a Management Review Board that is not utilized, nor does it take into account that the CIO participates in regular (currently weekly) meetings with the Deputy Secretary.

With the foregoing in mind, Recommendation 1 to "Reorganize the CIO position to have a direct reporting relationship to the Deputy Secretary and independent of ASAM" is not accepted. This is not a useful nor practical recommendation for the improving DOL's IT Governance.

Recommendations 2 through 5, which will be managed and executed by the OCIO and OASAM are accepted. These recommendations are in line with the intent of FITARA and will allow the Department to continue its IT transformation. OASAM/OCIO and other DOL Agencies will build a plan for their implementation at a pace that maintains program priorities, pandemic response, and hiring activities. This plan will be provided to OIG by the second quarter of 2022.

cc: Larry D. Turner, Acting Inspector General
Rachana Desai Martin, Assistant Secretary for Administration and Management
Gundeep Ahluwalia, Chief Information Officer

APPENDIX C: ACKNOWLEDGEMENTS

The audit team included:

Benjamin Brady, IT Specialist
Victor Chan, Auditor
Brian A. Devaney, IT Audit Manager
Lisa Finnican, Attorney
Stephen Fowler, IT Audit Director
Nathan Pike, IT Specialist
Naomi Reynolds, Auditor

**REPORT FRAUD, WASTE, OR ABUSE
TO THE DEPARTMENT OF LABOR**

Online

<http://www.oig.dol.gov/hotline.htm>

Telephone

(800) 347-3756 or (202) 693-6999

Fax

(202) 693-7020

Address

Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue, NW
Room S-5506
Washington, DC 20210