U.S. Department of Labor

Office of Inspector General—Office of Audit

REPORT TO THE OFFICE OF THE CHIEF INFORMATION OFFICER

CYBER SECURITY PROGRAM IMPROVEMENTS ARE NEEDED TO BETTER SECURE DOL'S MAJOR INFORMATION SYSTEMS

Date Issued:	March 31, 2015
Report Number:	23-15-001-07-725

U.S. Department of Labor
Office of Inspector General
Office of Audit

BRIEFLY…

Highlights of Report Number 23-15-001-07-725, issued to the Chief Information Officer for the Department of Labor.

WHY READ THE REPORT

The Federal Information Security Management Act (FISMA) of 2002 required federal agencies to implement information security programs and practices to secure its information and information systems.

This report provides information about DOL's Cyber Security Program and identifies four information security significant deficiencies, which have the potential to impact the Department's confidentiality, integrity and availability of labor information.

WHY OIG CONDUCTED THE AUDIT

The Federal Information Security Management Act (FISMA) of 2002 requires federal agencies to independently evaluate their information security programs and practices every year. As such, we conducted an audit to determine if DOL and its component agencies implemented the NIST information security controls required by the FISMA legislation.

READ THE FULL REPORT

To view the report, including the scope, methodologies and full agency response, go to:

http://www.oig.dol.gov/public/reports/oa/2015/23-15-001-07-725.pdf.

March 2015

CYBER SECURITY PROGRAM IMPROVEMENTS ARE NEEDED TO BETTER SECURE DOL'S MAJOR INFORMATION SYSTEMS

WHAT OIG FOUND

The OIG found DOL and its component agencies had not implemented the minimum NIST security controls, which presented unnecessary risks to the confidentiality, integrity, and availability of DOL's information, including personally identifiable information.

Our analysis of the NIST security controls not implemented by DOL identified significant deficiencies in four areas of DOL's cyber security program: 1) oversight and monitoring of information systems operated for DOL by third parties; 2) information system vulnerability and configuration management; 3) contingency planning and disaster recovery; and 4) access management.

WHAT OIG RECOMMENDED

We recommended the Chief Information Officer establish third-party oversight/monitoring processes and tools, increase the OCIO's oversight, testing, and verification of the identified significant deficiencies, and conduct better oversight of DOL's information technology asset and incident response management areas.

The CIO generally agreed with our recommendations, but disagreed with the OIG's determination that the identified deficiencies rise to the level of a significant deficiency at the department level. The CIO identified actions taken to remediate two of the five recommendations and stated that plans of actions and milestones were developed to remediate the other three recommendations.

Table of Contents

Exhibit

Appendices

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210

March 31, 2015

Inspector General's Report

Dawn M. Leaf
Chief Information Officer
U.S. Department of Labor
200 Constitution Ave, NW
Washington, DC 20210

Congress, the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and the Government Accountability Office have identified the information security of federal agencies as a continuing area of high risk. To ensure federal information assets are properly secured, Congress passed the Federal Information Security Management Act (FISMA) in 2002, which requires all executive agencies to use National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 200 and Special Publication (SP) 800-53 to protect their information and information systems, including those information systems provided or managed by third parties or accessed by other users with privileged access to federal data. FISMA also requires federal agencies to independently evaluate their information security programs and practices every year. Within the Department of Labor (DOL), the Chief Information Officer (CIO) has been designated by the Secretary and required by the Clinger-Cohen Act to ensure DOL and its component agencies have implemented the required security controls designed to thoroughly protect all DOL information technology assets.

This report presents a composite view and analysis of our Fiscal Year (FY) 2014 information security testing and results to answer the following question:

> Did DOL and its component agencies implement the minimum NIST information security controls required by FISMA legislation?

DOL's cyber security program needs improvement to meet the required minimum NIST information security controls we tested. Deficiencies were found in multiple DOL systems that resulted in unnecessary risks to the confidentiality, integrity, and availability of DOL's information, including personally identifiable information. Our analysis of these individual deficiencies found that, when taken collectively, significant deficiencies existed in four areas of DOL's cyber security program: 1) oversight and monitoring of information systems operated for DOL by third parties; 2) information system vulnerability and configuration management; 3) contingency planning and disaster recovery; and 4) access management.

DOL has 67 major information systems. During FY 2014, we tested information security controls for 3 DOL major information systems and DOL's entity-wide controls using the OMB/DHS metrics, NIST guidance, and DOL policies and procedures. Our analysis also included results from the testing of information security controls for 12 DOL major information systems conducted as part of DOL's FY 2014 financial statement audit. Our analysis identified 79 individual deficiencies involving information security controls that had not been implemented or were not operating as designed. We also performed follow-up testing on prior-year information security recommendations.

In addition to the significant deficiencies identified above, we also identified other areas of concern that warrant management attention and action, even though the areas were not considered significant deficiencies. These areas included Information Technology Asset Management, and Incident Response.

We communicated our concerns to major information system owners and agency management with Statements of Fact and Management Reports detailing our results and recommendations (see Exhibit 1).

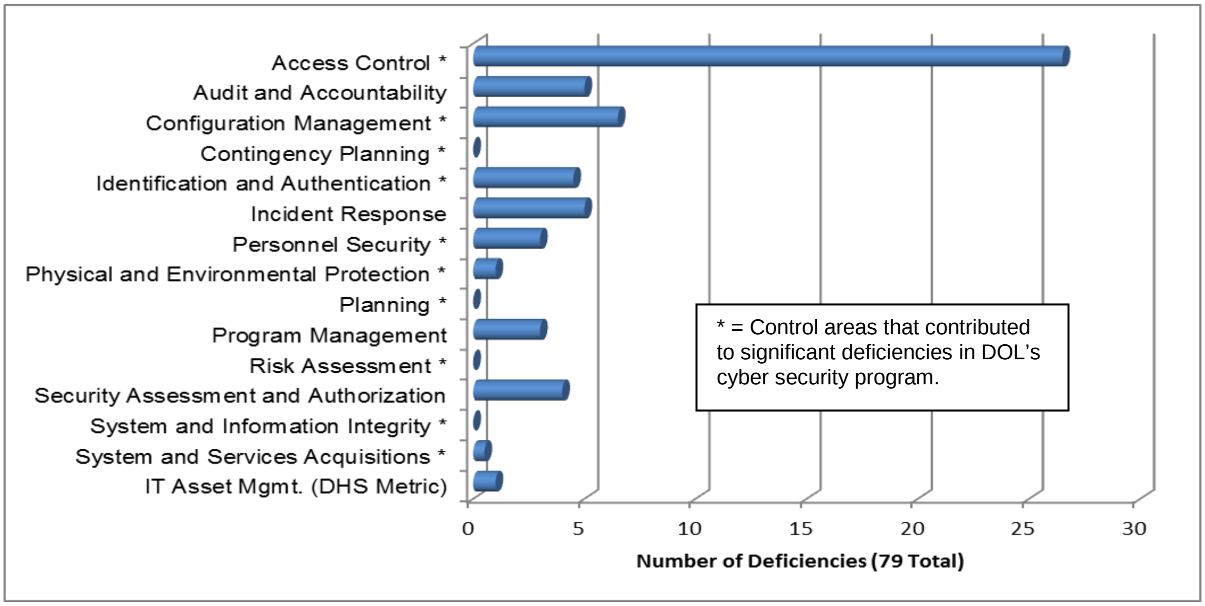
The CIO's response to our draft report has been incorporated within each appropriate section of the report and is included in its entirety in Appendix D.

RESULTS

Objective - Did DOL and its component agencies implement the NIST information security controls required by FISMA legislation?

Based on the major information systems and specific controls we tested, DOL and its component agencies had not implemented the minimum NIST security controls. Using the OMB/DHS FY 2014 Inspector General FISMA Reporting Metrics and NIST SP 800-53, we tested selected information security controls in the DOL cyber security program for the following 15 control areas: Access Control, Audit and Accountability, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Personnel Security, Physical and Environmental Protection, Planning, Program Management, Risk Assessment, Security Assessment and Authorization, System and Information Integrity, System and Services Acquisitions, and IT Asset Management. Our testing identified 79 individual deficiencies resulting from information security controls not implemented or not operating as designed (see Figure 1).

Figure 1: Areas of Security Control Deficiencies



We performed an analysis of the 79 individual deficiencies to determine if any of the deficiencies separately, or taken as a whole, were significant deficiencies requiring management's immediate attention. Our significant deficiency analysis and determinations were based on the following OMB criteria (see Table 1):

Table 1: Significant Deficiency Analysis Questions

Potential Weakness	**Significant Deficiency Workflow: Move through questions 1-5 in order. If any question results in a "Y" (yes) answer, answer question 6.**					
	1. Is this a design flaw? (Y/N)	2. Was this deficiency identified across multiple systems? (Y/N)	3. Does the deficiency compromise the security of the agency's information and/or information system? (Y/N)	4. Does this deficiency compromise the security of the agency's personnel? (Y/N)	5. Does this deficiency compromise the security of the agency's other resources, operations, or assets? (Y/N)	6. Would a prudent official conclude that the deficiency is at least a significant deficiency? (Y/N)

From our analysis of the 79 individual deficiencies, we identified 4 areas in DOL's cyber security program that, taken as a whole, were significant deficiencies and require management's immediate attention. The results of each significant deficiency are summarized below and are described in detail in Section A of the report.

1. Third-Party Oversight / Monitoring – DOL did not effectively implement oversight and monitoring tools specific to third-party service providers. As a result, DOL did not identify multiple areas of control deficiencies and the

need for immediate corrective actions, placing third-party DOL systems at risk.

2. Vulnerability and Configuration Management – DOL did not effectively implement Configuration Management and System and Information Integrity controls, which left DOL's information systems vulnerable to potential unauthorized access, service interruptions, and malicious technical attacks.

3. Contingency Planning / Disaster Recovery – DOL did not test contingency plans and did not develop or incorporate information technology needs and issues into disaster recovery plans, putting recovery in jeopardy and potentially delaying critical mission-systems from functioning in the aftermath of a disaster.

4. Access Management – DOL did not effectively implement Access Management, Identification and Authentication, and Audit and Accountability controls, which hindered DOL's ability to identify and validate users and control their access to DOL information and information systems.

These areas of significant deficiencies resulted in unnecessary risks to the confidentiality, integrity, and availability of DOL's information, including personally identifiable information.

DOL has already taken corrective actions related to contingency planning / disaster recovery. To mitigate the risks related to the remaining significant deficiencies, management needs to take immediate corrective actions to prevent unauthorized and unnecessary access to DOL data and eliminate known information system deficiencies identified in our testing.

A. Significant Deficiencies in DOL's Cyber Security Program

Third-Party Oversight / Monitoring

Oversight of third parties that either own and operate information systems on behalf of DOL or operate DOL-owned information systems was identified as a significant deficiency in prior years. In FY 2014, our testing of three major information systems operated on behalf of DOL identified controls that were not operating as intended and an overall lack of monitoring of the third-party service providers in two of those major information systems. These control deficiencies occurred because DOL had not designed specific testing and monitoring policies or procedures to help DOL information system owners, designated approving authorities, and contracting staff to ensure third-party service providers complied with minimum federal and DOL information-security requirements. DOL's Computer Security Handbook lacked specific guidance on how to monitor the oversight of third parties who own, operate, or support information systems on behalf of DOL.

If DOL does not provide guidance to designated personnel and monitor the oversight of these third-party information systems, the risk increases that the information systems' security postures would not be consistently reported to the authorizing officials who are responsible for ensuring adequate security exists and the information systems are operating to expectations.

Our testing identified that the following information security controls were not operating as intended and found an overall lack of monitoring of the third-party service providers for two major information systems:

System 1

- Access Controls – Separated user accounts were not removed in a timely manner. Users were granted privileged access without proper supervisor approval and rules of behavior acceptance. Account management, account recertification, and segregation of duties policies and procedures were not established, implemented, or documented.

- Identification and Authentication – Identification and Authentication policies and procedures were not established, implemented, or documented.

- System and Services Acquisition – Management could not provide evidence of monitoring performed in FY 2014 over third-party compliance with required DOL information security controls related to System 1.

System 2

- Access Controls – Personnel with access to approve promotion changes to production also had read and write access to the DOL source code development environment. The contractor had not developed procedures around segregation of privileged access to the operating system and the database. One contractor administrator had privileged access in both the operating system and database environment, which is not permissible according to DOL Policy. Also, user accounts were not disabled timely or lacked evidence of approval prior to disabling. For example, we found a disabled account had been accessed inappropriately 52 days after the account end date.

- Identification and Authentication – The database password configuration was not configured to require both upper case and lower case letters and, therefore, did not meet DOL password complexity requirements.

- Configuration Management – DOL and the contractor did not maintain a complete and accurate listing of application program changes.

- Contingency Planning – Functional testing of the information system restoration procedures was not performed in FY 2014.

The OCIO has continued to address issues related to the Third-Party Oversight/Monitoring deficiency through its risk mitigation strategy and changes to the DOL Computer Security Handbook, which provides policy and guidance to implementing information security in all DOL information systems that are owned by DOL or operated by a third party. These actions notwithstanding, the recurring nature of these deficiencies demonstrates the OCIO has not effectively implemented controls related to the Third-Party Oversight / Monitoring.

Based on the aggregation of the results above, we determined the area of Third-Party Oversight/Monitoring is a significant deficiency. Deficiencies were identified across two major information systems and have the potential to impact other information systems and resources. Furthermore, these deficiencies create potential risks to the major information systems' confidentiality, integrity and availability.

RECOMMENDATION

1. We recommend the Chief Information Officer establish third-party oversight/monitoring processes and tools that guide information system owners on how to better monitor third-party service providers' effectiveness in implementing NIST information security requirements and Administration priorities.

The CIO agreed additional guidance on monitoring security compliance of third parties was needed and the OCIO developed additional guidance. The CIO stated the guidance is in draft and planned to be issued in the third quarter of FY 2015. The OIG plans to follow up on the CIO's planned corrective actions in the following fiscal year.

Vulnerability and Configuration Management

We identified deficiencies in 13 of the 15 major information systems tested in the Risk Assessment, System and Information Integrity, and Configuration Management security control families. Information security controls were not operating as intended to maintain and monitor the integrity of information systems through the implementation of a process for timely and secure installation of software patches and remediation of configuration related vulnerabilities.

Vulnerability Scanning and Flaw Remediation are complementary controls that address vulnerability assessment testing in performing scans and addressing corrective actions. Strong Vulnerability Scanning, Flaw Remediation and Configuration Management control practices reduce the risk of system exposure to known deficiencies, malicious technical attacks, and unauthorized or unintentional changes.

Specifically, we identified 20 deficiencies within the Risk Assessments (3), System and Information Integrity (10), and Configuration Management (7) control families (see Table 2).

Table 2: Vulnerability and Configuration Management Deficiencies Identified

NIST Criteria	Control Name	Number of Deficiencies and System(s)
3 Risk Assessment Deficiencies		
RA-5	Vulnerability Scanning	3 Deficiencies in 3 systems
10 System and Information Integrity Deficiencies		
SI-2	Flaw Remediation	10 Deficiencies in 9 systems
7 Configuration Management Deficiencies		
CM-2	Baseline Configurations	2 Deficiencies in 2 systems
CM-3	Configuration Change Control	2 Deficiencies in 2 systems
CM-5	Access Restrictions for Change	1 Deficiency in 1 system
CM-6	Configuration Settings	2 Deficiencies in 2 systems

Based on analysis of the results above, we determined the area of Vulnerability and Configuration Management, taken as a whole, is a significant deficiency. Program agencies had taken some corrective actions for the areas noted above to mitigate the information system-level deficiencies. While the OCIO's efforts to reduce the number of deficiencies continued, those efforts were not sufficient enough to reduce risks to an acceptable level since the deficiencies identified occurred across multiple major information systems and have the potential to impact other resources. Furthermore, without increased oversight over mitigation and testing activities, these deficiencies create the potential for risks to the major information systems' confidentiality, integrity, and availability.

RECOMMENDATION

2. We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to the Vulnerability and Configuration Management Significant Deficiency.

The CIO's response indicated it already performs a number of oversight activities and planned supplementing those activities with additional automated continuous monitoring tools. The OIG plans to follow up on the CIO's actions taken in the following fiscal year.

Contingency Planning / Disaster Recovery

We identified deficiencies in Contingency Planning/Disaster Recovery for 6 of 15 major information systems tested and the entity-wide program, including issues with Developing a Contingency Plan, Contingency Plan Testing, and Information System Backup. The testing identified incomplete entity-wide contingency planning, incorrect or out-of-date contingency plans, untested system backups, and insufficient contingency plan testing.

Effective planning and prioritization of essential information systems and processes enables organizations to recover from disasters and operate without excessive interruption. Furthermore, testing the contingency plan is vital to determine the effectiveness of the plan. Identifying deficiencies in the plan and training relevant staff to carry out the plan must take place before it is activated in response to a disaster or information system compromise.

Developing a Contingency Plan

Entity-wide Contingency Planning

We were informed by DOL that the entity-wide contingency plan and disaster recovery deficiency identified in FY 2013 was being monitored and remediated through the tracking of a Plan of Action and Milestones (POA&M), and as of July 2, 2014, the POA&M was “in progress” and had a due date of September 30, 2014. Therefore, we determined the prior-year finding remained open and a deficiency to DOL’s cyber security program through FY 2014.

The inability to develop a comprehensive entity-wide Contingency Plan and Disaster Recovery Process to integrate information technology interests within the contingency plan increased the risk that unnecessary delays in the recovery of critical information resources will affect the restoration process. It is important to ensure information systems and data sets are prioritized in such a way that essential functions receive the necessary resources to operate effectively in the event of a disaster. Lack of prioritization of information systems may affect the restoration process and may cause unnecessary delays in the recovery of critical information resources.

On December 5, 2014, after the reporting period, the Assistant Secretary for Administration and Management provided documentation demonstrating the completion of actions required to address this issue, as follows:

- Conducted Business Impact Analysis workshops for agencies

- Received and reviewed completed and signed Business Impact Assessments

- Reviewed and signed agency information technology and information system disaster prioritization lists

- Prioritized and obtained Executive management approval of the department-level recovery sequence

- Developed and delivered to Executive management a DOL-wide Information Technology Disaster Recovery Plan

Based on review of the information provided, this deficiency has now been corrected; however, for the reporting period (FY 2014), this remained a significant deficiency.

Contingency Plan Testing

We identified deficiencies in 6 of 15 major information systems tested. These deficiencies included untested backups, limited contingency plan testing, and incorrect contingency plan information.

Contingency Plan testing addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Effective planning can support the timely recovery of essential processes enabling organizations to operate without excessive interruption. Furthermore, testing the contingency plan is vital to determine the effectiveness of the plan and to identify potential deficiencies in the plan. Identifying deficiencies in the plan and training relevant staff to carry out the plan must take place before it is activated in response to a disaster or information system compromise.

Information System Backup Results

Testing indicated that 2 of 15 major information systems tested did not perform information system backups in a timely manner. The backup configuration for one major information system did not include two servers. In addition, for the same major information system the other servers were not successfully completing the backups. The other major information system had two production servers added, which were not backed up as this is an inherited control and lack of oversight of the third-party performing work allowed this to occur.

Information system backup addresses information system restoration in the event that the information systems are compromised. Performing information system backups at a frequency established and agreed upon by agency management is essential to ensuring data residing within the information system can be restored in the event that data is lost or corrupted.

Management for both major information systems represented that corrective action plans to remediate these deficiencies were completed or scheduled to be completed by the second quarter of FY 2015. The action plans included performing complete backups and reviewing and modifying the process to ensure servers needing backup are not overlooked.

Without performing information system backups in a timely manner, the agency runs an increased risk that data residing within the information system may not be restored in the event that data is corrupted or lost, compromising the availability and integrity of the agency information system data. Furthermore, agency management could be unable to perform a full restore of the major information systems following a major disaster, which could affect the agencies' ability to carry out its mission.

Limited Contingency Plan Testing and Incorrect Contingency Plan Information

Testing indicated 5 of 15 major information systems performed inadequate testing of the contingency plans. Our work identified one major information system that had never been fully tested, one major information system did perform testing, and two other major information systems did not complete testing during FY 2014 as required. In addition, the contingency plans tested had incorrect or outdated information and one major information system failed to provide results to management for review as required.

Information system backup addresses information system restoration in the event systems are compromised. Performing information system backups at a frequency established and agreed upon by agency management is essential to ensuring data residing within the information system can be restored in the event that data is lost or corrupted.

Management for two major information systems represented that corrective action plans to remediate these deficiencies were completed or scheduled to be completed by the second quarter of FY 2015. The action plans included performing complete testing of the backup process, reviewing and modifying the backup schedules, and including management review as part of the backup process. Management represented DOL's corrective actions pertaining to a prior-year's recommendation related to DOL-wide Information Technology Disaster Recovery Plan were not completed until FY 2015. However, the Contingency Planning / Disaster Recovery deficiencies as a whole remained a significant deficiency during FY 2014.

RECOMMENDATION

3. We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to Contingency Planning / Disaster Recovery.

The CIO's response described prior difficulties performing adequate testing during the year and planned to ensure full testing would be a focus in FY 2015. The OIG plans to follow up on the CIO's actions taken in the following fiscal year.

Access Management

We concluded Access Management was a significant deficiency in the DOL cyber security program and that it warranted heightened management attention. In FY 2014, we again identified Access Management as an area of continued deficiency as we reported Access Management (AC), Planning (PL), and Personnel Security (PS) controls were not operating as intended to prevent unauthorized and unnecessary access to 13 of 15 major information systems and to the entity-wide process.

Strong Access Management controls would prevent unauthorized and unnecessary access to the data contained within DOL information systems.

The Access Management analysis consisted of 30 Access Management deficiencies, 7 Identification and Authentication deficiencies, and 6 Audit and Accountability deficiencies, as illustrated in the following table (see Table 3).

Table 3: Access Management Deficiencies Identified

NIST Criteria	Control Name	Number of Deficiencies and Major Information Systems
30 Access Management Deficiencies		
AC-2	Account Management (Automated System Account)	16 Deficiencies in 11 systems
AC-5/ AC-6	Separation of Duties/ Least Privilege	5 Deficiencies in 4 systems
PL-4/ PS-6	Rules of Behavior / Access Agreements	9 Deficiencies in 7 systems
7 Identification and Authentication Deficiencies		
IA-2/ IA-5	Identification and Authentication of Organizational Users / Authenticator Management (Shared Accounts, Password Settings, and Personal Identity Verification)	7 Deficiencies in 4 systems and the Entity-Wide program
6 Audit and Accountability Deficiencies		
AU-6	Audit Review, Analysis, and Reporting	6 Deficiencies in 6 systems

<u>Access Management</u>

The 30 Access Management deficiencies identified above occurred in 12 of the 15 major information systems and included deficiencies related to Account Management, Separation of Duties, Least Privilege, Rules of Behavior, and Access Agreements security controls.

These controls, when properly designed and implemented, ensure protection of information systems from the abuses of inappropriate access by allowing only authorized individuals to have access to the information systems and information. These controls also appropriately limit the scope of authorized individuals' access so it is commensurate with their roles and responsibilities.

Account Management Testing

We identified ten major information systems and one data center with accounts still active after individuals' separation dates, including four major information systems that had user accounts accessed after those users were separated. Removing access to unneeded accounts reduces the risk of unauthorized access. Accounts for these users were either currently active as of testing or had been active for periods after the users' separation dates. The following table helps provide perspective on the extent of how long the accounts remained inappropriately active, and the identified condition has been an issue (see Table 4).

Table 4: Active Accounts after User's Separation

Major Information System	Accounts Active After Separation	Days Active After Separation	Accounts Accessed After Separation	First Time Issue Reported
System 1	88	16 to 354	2	N/A
System 2	89	38 to 220	2	FY 2008
System 3	7	2 to 150	3 (3 to 27 days)	FY 2004
System 4	1	21	0	FY 2008
System 5	3	13 to 33	0	FY 2009
System 6	5	2 to 67	N/A	FY 2011
System 7	13	3 to 426	N/A	FY 2006
System 8	6	2	N/A	FY 2013
System 9	2	34 and 48	N/A	N/A
System 10	85	3 to 34	1 (1 day)	FY 2007
Data Center	1	180	N/A	FY 2011

Management for nine major information systems generally represented that the agency was relying on increased awareness and training, along with changes to policies and procedures, to address the deficiencies. Management for two major information systems identified corrective actions with planned completion prior to September 30, 2014, and the remaining created POA&M items to address the deficiencies with planned completion in FY 2015.

Furthermore, we determined six major information systems were not disabling user accounts after 60 days of inactivity as required by the DOL Computer Security Handbook. By exceeding the required limit, inactive accounts older than 60 days run a greater risk of being exploited for unauthorized access to information contained on any information system available to the inactive user's prescribed access privileges.

For one major information system, the accounts that were not disabled after 60 days of inactivity remained accessible for periods of inactivity that extended beyond the limit from 1 to as many as 353 days (or 61 to 413 days of inactivity). Also, we identified 1,098 accounts that exceeded the required limit, including system administrator accounts.

We also found one major information system was not configured to disable accounts after 60 days of inactivity for users having privileged access on the servers supporting the major information system.

Management for six major information systems created POA&Ms to address the deficiencies with planned completion dates in FY 2015.

Separation of Duties / Least Privilege Testing

Our testing found 4 of 15 major information systems had separation of duties or concept of least privilege deficiencies. These types of deficiencies increase the risk of individuals performing commingled duties that together afford an employee unintended authority and unchecked opportunity for abuse, including, but not limited to, introducing fraudulent data or malicious code into the system.

Management for one major information system had not implemented policies or procedures over its system to ensure appropriate separation of duties. We also determined for three major information systems that the concept of least privilege was not followed, since system administrators were allowed to have access to both the operating system and database environments, which was a violation of DOL policy. In addition, we determined a developer for one major information system had access to both production and development processing environments.

Inadequate separation of duties and disregarding the concept of least privilege could allow the developer to create system modifications and promote them into production defeating the most basic procedural protections designed to ensure change control, or allow a privileged user to commit fraudulent transactions and then destroy evidence of the wrongdoing.

Management for two of the major information systems created POA&M items with planned completion in FY 2015 to address the deficiencies.

Rules of Behavior / Access Agreements Testing

We determined 7 of 15 major information systems had 9 deficiencies related to ensuring all required documents were completed prior to granting individuals access and maintained as required by the DOL Computer Security Handbook. Access authorizations with management approval were not maintained for six major information systems. Rules of Behavior documents were not maintained for five major information systems.

Without proper Access Management controls, as evidenced in the examples above, individuals, unauthorized or even authorized, have the ability to execute inappropriate transactions in the affected DOL major information systems.

Management for six major information systems created POA&M items with planned completion in FY 2015 to address the deficiencies. Management for two major information systems indicated corrective actions were completed by providing managers the correct forms to be used when granting access to their major information systems.

Identification and Authentication

There were seven Identification and Authentication deficiencies in 5 of 15 major information systems and in the entity-wide process (see Table 3). We identified deficiencies with the implementation of the Identification and Authentication and Authenticator Management controls regarding generic/shared accounts, password settings, and personal identity verification (PIV) in five major information systems, along with DOL entity-wide controls. Minimum baseline controls for Identification and Authentication and Authenticator Management are established to make all user accounts accountable to an individual or process, verify who is accessing the system, and provide validity of transactions (non-repudiation) and accountability for actions performed.

Generic/Shared Accounts Testing

We identified generic and shared account deficiencies for 2 of the 15 major information systems tested. We identified 1 generic active account for one major information system, 59 generic accounts for a second major information system, and the second system included developers who were sharing a system account that allowed them to read, modify, and delete data on the production server. We also determined the second systems’ database administrators shared an account on the production server and the first system had a shared account on a network device.

DOL policy clearly prohibits the use of generic and shared accounts. Unique user accounts provide the ability to identify and hold accountable an individual for the actions taken from the account or process.

Both major information system owners created POA&Ms, with planned completion in FY 2015, to address the deficiencies and started reviewing and removing the generic / shared user accounts.

Password Configuration Settings Testing

We found password configuration setting deficiencies for 2 of the 15 major information systems tested.

This control establishes parameters (i.e., password composition, length, life, history) that the information system uses to identify who is accessing the information system. These settings ensure complexity and change requirements are enforced to increase the difficulty of gaining access through guessing or deciphering another user's password.

- System 1: The servers and database had password settings of a minimum password life of 0 – 7 days, which does not meet the DOL CSH standard of 15 days. The required setting prevents a user from changing the password again before 15 days have elapsed since the last change. A shorter time could allow an unauthorized change to a password. Configuring a longer minimum password age helps to ensure a password history control is effective. Without a sufficiently long minimum password age, users could cycle through passwords repeatedly until they got to an old favorite, thus defeating the intent of the password history control.

  Once the auditors alerted management for system 1 about this condition, system managers created a POA&M item and initiated corrective actions with planned completion in FY 2015.

- System 2: The database password configurations were not configured in accordance with the DOL Computer Security Handbook.

  Management indicated they were in the process of switching service providers and that they would address the deficiency in FY 2015.

Personal Identity Verification Testing

According to the FY 2014 FISMA Reporting Metrics, the expected level of performance was 75 percent of users utilizing PIV cards for identification and authentication. While DOL used PIV cards for physical access, it did not enforce required use of PIV cards for logical access to any DOL major information system and did not meet the target for FY 2014. DOL component agencies were waiting for the OCIO to implement its corrective action plan for PIV implementation.

We reported the Identification and Authentication deficiency in FY 2013, noting DOL had not used PIV for logical access as required by federal mandate and did not have a viable plan for implementation. During FY 2014, OCIO management agreed DOL had not yet implemented a logical access control system enabling and requiring users to logon using their PIV card and PIN for any of the DOL major information systems.

While most DOL employees have been issued PIV cards, not using these PIV cards for logical access defeats a primary purpose of the card, which is to ensure security of federal information systems and information by providing for interoperability and trust in allowing logical access to federal information systems, networks, and resources on a government-wide basis.

OCIO's management stated DOL has a detailed implementation plan that will leverage the General Services Administration's USAccess solution, enabling DOL to comply with HSPD-12 requirements for mandatory PIV card logon once all DOL employees and contractors migrate to the USAccess solution.

Identification and Authentication control deficiencies impact the confidentiality and integrity of DOL's information and information systems by increasing the risk of unauthorized systems access, unauthorized infrastructure access, and unauthorized privileges. These Identification and Authentication control deficiencies also reduce DOL's ability to provide validity of transactions (non-repudiation) and accountability for actions performed.

Audit and Accountability

We identified Audit and Accountability control deficiencies for 6 of the 15 major information systems tested. We identified a lack of documented audit log reviews.

This monitoring control provides the process for identifying incidents, problems, and deficiencies in an information system to correct such issues and is necessary to protect information resources from harm or misuse. Without effective ways to gather audit logs or review them timely, systems bear an increased level of risk from fraudulent actions that might compromise data. Without proper and timely review of audit logs, risks increase that anomalies and security-related incidents go unnoticed and uninvestigated, thereby jeopardizing data from DOL information systems.

Management for one major information system acquired a log aggregate tool for its system. However, the staff stopped performing reviews of the logs even though the tool to aggregate the audit logs from the system resources was operational. For the other systems, audit logs were not documented for a selection of dates tested.

Management for two major information systems created POA&Ms to implement or enhance current policies and procedures to ensure the review of audit logs are documented with planned completion in FY 2015.

Based on the analysis of the results above, we determined the area of Access Management was a significant deficiency in the DOL cyber security program during the tested period. While management for two agencies have been taking the corrective actions noted above to address the system-level deficiencies, the OCIO's efforts to reduce the number of these deficiencies are not yet sufficient to bring about an acceptable level of risk. These deficiencies were across multiple systems and have the potential to impact other resources. Further, without increased oversight over mitigation and testing activities these deficiencies create the potential for risks to information systems' confidentiality, integrity, and availability.

RECOMMENDATION

4. We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to Access Management.

The CIO's response to our draft report stated that the Identity and Access Management program (IAM) was not fully funded. The CIO stated that DOL planned to fully implement IAM during the first quarter FY 2016, contingent upon budget approval. The OIG plans to follow up on the CIO's planned corrective actions in FY 2016.

B. Other Deficiencies Warranting Management Attention

Through Statements of Fact, we also identified and reported deficiencies in Information Technology Asset Management and Incident Response. These deficiencies resulted from a lack of compliance with the NIST system controls required by FISMA legislation. While these deficiencies were not at the level of a significant deficiency in the DOL cyber security program, the deficiencies do warrant management attention and action because of the exposure these present to DOL.

Information Technology Asset Management

We determined the OCIO inventory entity-wide list maintained by the Office of Administrative Services was manually maintained and only tracked hardware. Also, there was no current enterprise-wide automated Information Technology Asset Management system in place that could monitor and maintain a complete, accurate, and readily-available listing of the hardware and software inventory of DOL. Specifically, although an Information Technology Asset Management system had been implemented, the process to update the annual FISMA-related inventory was a manual data call, which did not include software licensing information, as required by the DOL Computer Security Handbook.

Proper hardware and software inventory management helps organizations manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources. Organizations that develop and maintain an effective information technology asset-management program further minimize the incremental risks and related costs of advancing information technology portfolio infrastructure projects based on old, incomplete, or less accurate information. Further, failure to maintain an accurate inventory of DOL hardware, software, and firmware can result in misused or misplaced assets, which can compromise the confidentiality and integrity of information system data.

OCIO's management stated DOL's automated system did not have the appropriate reporting capabilities to maintain a complete, accurate, and readily-available listing of the hardware and software inventory. Further, OCIO management contended DOL met the departmental FISMA data submission requirements for asset management as requested by OMB without issue and that the requirement for full automation of all processes to complete an inventory is not required for DOL and is not possible with current DOL capabilities. In addition, inventory processes of all information technology assets require some manual intervention along with automation in order to maintain an accurate inventory. OCIO management stated it will continue to research methods and technologies that will enhance the current processes in place for DOL's full information technology assets tracking and management.

While OCIO management describes a mixed process to create an information technology asset inventory, the lack of an enterprise-wide, automated asset management system, as required, can hinder the OCIO's ability to monitor DOL information systems as a whole.

Incident Response

We determined incidents were not reported to the DOL Computer Security Incident Response Center (CSIRC) and subsequently to the United State Computer Emergency Readiness Team (US-CERT) within the timeframes required by the DOL Computer Security Handbook and US-CERT for 4 of 5 major information systems tested.

Specifically, we identified the following:

- System 1 personnel did not report two category-1 incidents and one category-4 incident to DOL's CSIRC within the required reporting timeframes.

- System 2 personnel did not report 1 of 2 identified incidents to DOL's CSIRC. Furthermore, 3 of the 5 breaches management for System 2 reported to DOL's CSIRC were not reported within US-CERT and DOL-required timeframes for a category-1 incident.

- System 3 personnel did not report 2 of 7 category-1 incidents selected for testing to DOL's CSIRC within the DOL Computer Security Handbook required timeframes.

- System 4 personnel did not complete the POA&Ms created to remediate a FY 2013 incident response finding where 1 of 4 incidents was not reported to DOL's CSIRC within the required DOL Computer Security Handbook reporting timeframes.

- DOL's OCIO personnel did not report 1 of 8 selected incidents to US-CERT within the timeframe required by the DOL Computer Security Handbook and US-CERT.

Attacks frequently compromise data and it is critical to respond quickly and effectively when security breaches occur. Without having developed and implemented a coordinated approach to incident response, DOL agencies would be at risk of loss or theft of information, including personal and private student information, and disruption of services caused by incidents.

Management for System 1 stated that due to the time it took to confirm the reported incident and obtain the appropriate documentation, they missed the reporting timeframe for a category-1 incident. Management noted the original details did not indicate that the incident involved potential unauthorized access. Management for System 2 stated their contractor did not follow documented incident response procedures. Management for System 2 also stated it reported all category-1 incidents to OCIO within one hour as required by DOL policy. Management for System 3 stated a POA&M had been created to track the remediation of this finding.

OCIO management stated an incident as reported by System 2 management required additional investigation before it was reported to US-CERT. OCIO management stated this delay in reporting was caused by system management incorrectly classifying the incident. OCIO management further stated that once the correct classification was determined and assigned to the incident, it was reported to US-CERT within an hour, as required for category-1 incidents.

While we recognize DOL conducted further due diligence to ascertain the severity of the incident, the initial notification of the incident characterized it as involving a potential disclosure of a confidential survey participant's identity. This initial notification should have signaled to DOL the incident was, at the time, a category-1 incident and should have been reported to US-CERT within the one hour timeframe.

Reporting missteps by the program agencies and the OCIO's lack of coordination efforts resulted in the program agencies not reporting incidents as required. Failure to report incidents within the designated timeframe can result in an untimely response to critical incidents and can potentially leave DOL and its agencies vulnerable to further unauthorized access or attacks.

RECOMMENDATION

5. We recommend the Chief Information Officer conduct better oversight of DOL's information technology asset and incident response management areas to prevent unauthorized and unmanaged devices from handling DOL information and to ensure all incidents are timely reported to CSIRC and US-CERT.

The CIO's response stated several incident response training sessions had taken place in FY 2014 and FY 2015. To further reinforce the area of incident response, the OCIO is in the process of updating the DOL CSH Volume 8 to incorporate the new US-CERT reporting guidelines and training by the third quarter of FY 2015. OCIO management planned to continue researching methods and technologies that will augment the current processes for DOL's full IT assets tracking and management. The OIG plans to follow up on the CIO's planned corrective actions in FY 2016.

CONCLUSION

The significant deficiencies and other deficiencies identified in this report demonstrated DOL and its component agencies had not adequately implemented the minimum NIST information security controls required by FISMA legislation. The recurring deficiencies in Third-Party Oversight, Vulnerability and Configuration Management, Contingency Panning / Disaster Recovery, and Access Management, continued to expose DOL's mission-critical systems to potential harm, misuse of personal information, and disruption of critical information technology services. Implementation of the recommendations already presented in this report would reduce the risk these deficiencies present to the DOL cyber security program and its information and information systems. Collectively, the recommendations were:

1. We recommend the Chief Information Officer establish third-party oversight/monitoring processes and tools that guide information system owners on how to better monitor third-party service providers' effectiveness in implementing NIST information security requirements and Administration priorities.

2. We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to the Vulnerability and Configuration Management Significant Deficiency.

3. We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to Contingency Planning / Disaster Recovery.

4. We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of DOL's cyber security program related to Access Management.

5. We recommend the Chief Information Officer conduct better oversight of DOL's information technology asset and incident response management areas to prevent unauthorized and unmanaged devices from handling DOL information and to ensure all incidents are timely reported to CSIRC and US-CERT.

We appreciate the cooperation and courtesies DOL personnel extended to the Office of Inspector General during our work.

Elliot P. Lewis

Elliot P. Lewis
Assistant Inspector General
for Audit

Exhibit

Exhibit 1

FISMA Management Reports Issued

Agency	Report Number	Report Title
OASAM	23-14-017-07-727	Verification of OASAM Remediation Efforts of Prior-Year Information Technology Security Recommendations
BLS	23-14-019-11-001	Verification of BLS Remediation Efforts of Prior-Year Information Technology Security Recommendations
SOL	23-14-020-08-001	Verification of SOL Remediation Efforts of Prior-Year Information Technology Security Recommendations
BLS	23-15-002-11-001	FY 2014 FISMA: National Longitudinal Survey system Testing
ETA	23-15-003-03-370	FY 2014 FISMA: Job Corps LAN/WAN Testing
OLMS	23-15-004-04-421	FY 2014 FISMA: Electronic Labor Organization Reporting System Testing
OIG	23-15-005-09-001	Verification of OIG Remediation Efforts of Prior-Year Information Technology Security Recommendations
OCIO	23-15-006-07-725	Verification of OCIO Remediation Efforts of Prior-Year Information Technology Security Recommendations

Appendices

Appendix A

Background

Congress passed FISMA in 2002, which requires all executive agencies to use NIST FIPS Publication 200 and SP 800-53 to protect their information and information systems, including those systems provided or managed by third parties or accessed by other users with privileged access to federal data.

The Secretary of Labor sets priorities and provides guidance for the overall efforts of CIO programs. However, the primary objective of the CIO is to ensure DOL is operating in accordance with policies, procedures, and requirements of the federal government that relate to the security, implementation, and management of IT.

Under FISMA, the CIO is responsible for:

- Developing and maintaining a [DOL-wide] information security program;
- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;
- Ensuring agencies have trained personnel sufficient to assist [DOL] in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and
- Reporting annually and in coordination with DOL agencies' senior officials to the [Secretary of Labor] on the effectiveness of the agency information security program, including progress of remedial actions.

In DOL, the above duties and responsibilities of the CIO are implemented through the OCIO.

Appendix B

Objective, Scope, Methodology, and Criteria

Objective

Did DOL and its component agencies implement the minimum NIST information security controls required by FISMA legislation?

Scope

As part of our FISMA performance work, we assessed the effectiveness of selected information security controls in place for a subset of 3 major information systems within 3 agencies out of a total of 67 DOL major information systems[1] for 15 agencies. We selected a subset of DOL systems and NIST SP 800-53 Revision 4 control families using a risk-based approach for testing.

The scope of our testing included the information controls in place during the period of October 1, 2013, through September 30, 2014. We conducted our testing at the Frances Perkins Building in Washington, DC, and DOL data center sites.

The control tests included reviews of DOL agency policies and procedures for implementing and monitoring mandatory information security controls, as well as implementation of the mandatory controls for DOL agency systems. Based on OMB/DHS criteria, we tested the following security control areas: enterprise-wide continuous monitoring; security configuration management; access management; incident response and reporting; risk management; security training; remediation/POA&Ms; remote access; enterprise-wide business continuity/disaster recovery; third-party oversight; and security capital planning and investment.

In addition, our analysis and reporting on DOL's information security incorporated the results from the relevant testing and reporting of information security of DOL's financial systems. Twelve financial systems were included in our scope.

Furthermore, our work considered results from follow up of prior deficiencies.

Methodology

This project followed a phased development, including planning, testing, and reporting as discussed below.

[1] During planning, we used the major system inventory provided by the OCIO, which had 69 systems at that time. During the fiscal year, systems were added and retired. The OCIO reported 67 major information systems in the CIO's annual FY 14 FISMA reporting to the Labor Secretary.

Planning

We reviewed DOL's policies and procedures, as well as applicable federal laws, guidelines, and requirements. We obtained and examined DOL information security policies, procedures, and controls in place for the selected DOL major information systems, including related third-party systems, in order to gain an understanding of and a familiarity with the DOL information security control environment, and to facilitate the planned process of assessing both the effectiveness of selected information security controls, as well as the extent of DOL compliance with information security requirements and FISMA requirements.

In order to meet our responsibility to provide OMB with results regarding the effectiveness of DOL's cyber security program, and to apprise the OCIO concerning design and operating deficiencies identified under agency and DOL key information security controls, we needed to both summarize the work performed in answering the OMB IG Reporting Template, and provide additional information and analyses regarding information security deficiencies identified in DOL.

In determining the systems, we used a risk-based approach to select our subset of information systems from DOL's inventory of major information systems.

Control areas were tested based on the guidance outlined in the OMB Memorandum 15-01 entitled: Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices, which included: enterprise-wide continuous monitoring; security configuration management; access management; incident response and reporting; risk management; security training; remediation/POA&Ms; remote access; enterprise-wide business continuity/disaster recovery; third-party oversight; and security capital planning and investment.

Team discussions were held to consider possible fraud risk factors at DOL and its agencies. A fraud inquiry with DOL and agency management was conducted to consider fraud risk factors.

Testing

We conducted our testing through inquiry of agency personnel, observation of activities, inspection of relevant documentation, and performance of technical information security tests to obtain evidence for supporting our conclusions.

Our testing included controls based on the minimum recommended information security controls established by NIST FIPS Publication 200 and SP 800-53 Revision 4, OMB and the DOL Computer Security Handbook, and considered any compensating controls disclosed during inquiry, observation, or testing.

When necessary, we used random sampling to evaluate specific control elements within the areas of user account forms, separated users, and configuration management changes in the major information.

We tested data reliability by obtaining system-generated lists and evaluating source documentation provided to support system-generated data. Source documentation was compared to system-generated lists to determine the accuracy of that data.

Reporting

Upon completion of the system testing, we reported results to the agency official for the systems reviewed with recommendations based on the testing of security controls. Using those results and the results from testing of the financial systems, we aggregated the results and performed additional analysis described below and reported the results of the analysis and entity-wide issues in this report to the CIO.

We evaluated the results within a given control family, information system, or agency to determine if identified deficiencies had similar causes or similar risks. If an area of common security deficiency was identified with similar causes or risks, we performed an analysis of the aggregated results with related risks and cause to determine if these constituted a significant deficiency as defined by OMB Memorandum 15-01:

> A significant deficiency is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.

In planning and performing our work, we considered DOL’s internal controls that were relevant to our objectives by obtaining an understanding of those controls and by assessing control risk for the purposes of achieving our objectives. Our objective was not to provide assurance on the internal controls. Therefore, we did not express an opinion on the internal controls as a whole. Our consideration of DOL’s internal controls relevant to our objectives would not necessarily disclose all matters that might be reportable conditions. Because of the inherent limitations on internal controls, noncompliance may nevertheless occur and not be detected.

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

Criteria

OMB issued Memorandum 15-01 titled, "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices" to define the FISMA testing and reporting metrics for FY 2014.

We used the following criteria in the performance of our audit:

- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- FISMA of 2002
- NIST SP 800-53 Revision 4
- Department of Labor Manual Series 9 - Information Management
- DOL Computer Security Handbook

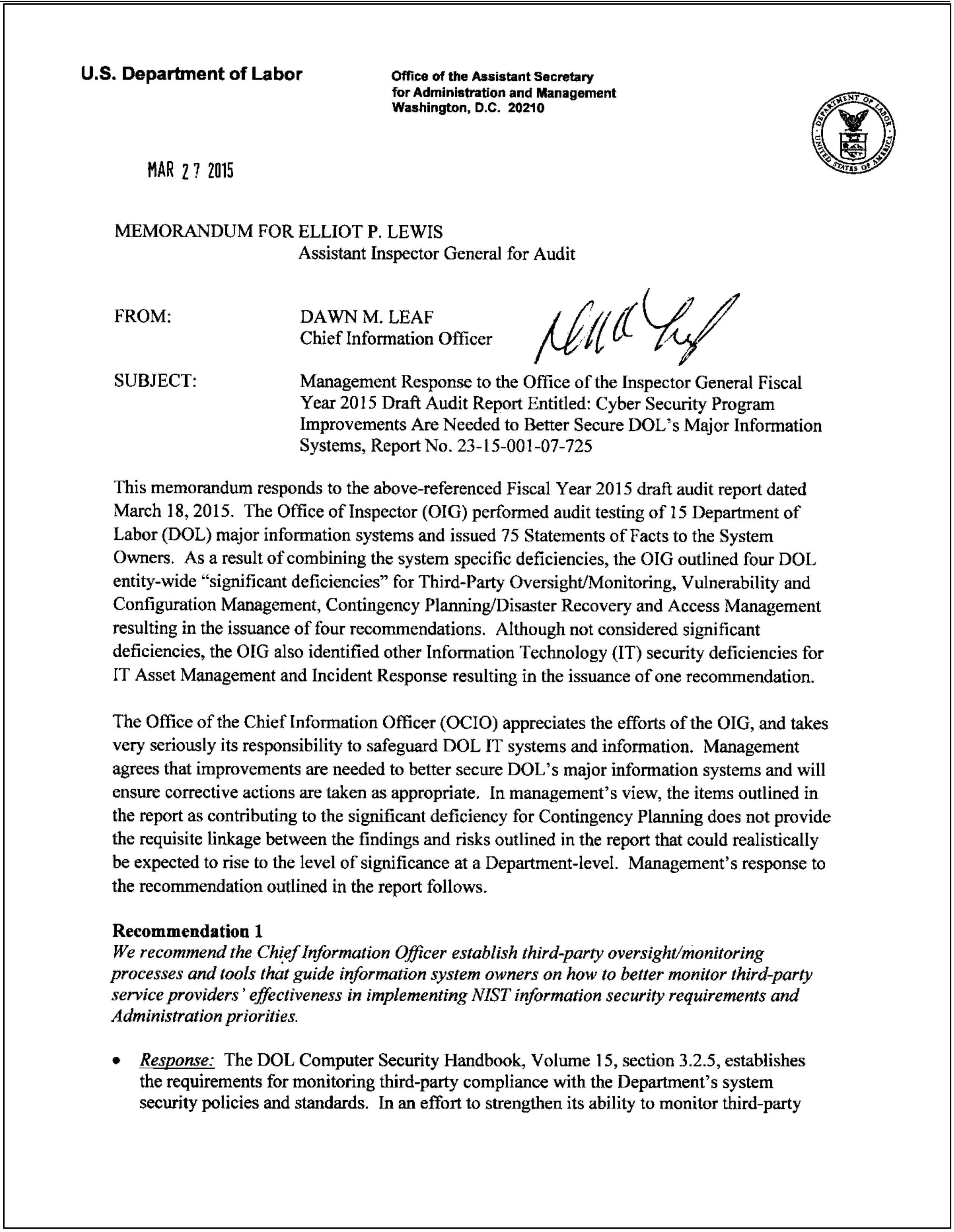
Appendix C

Acronyms and Abbreviations

CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
DOL	Department of Labor
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SP	Special Publication
US-CERT	United States - Computer Emergency Readiness Team

Appendix D

OCIO Response to Draft Report



U.S. Department of Labor

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

MAR 27 2015

MEMORANDUM FOR ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: DAWN M. LEAF
Chief Information Officer

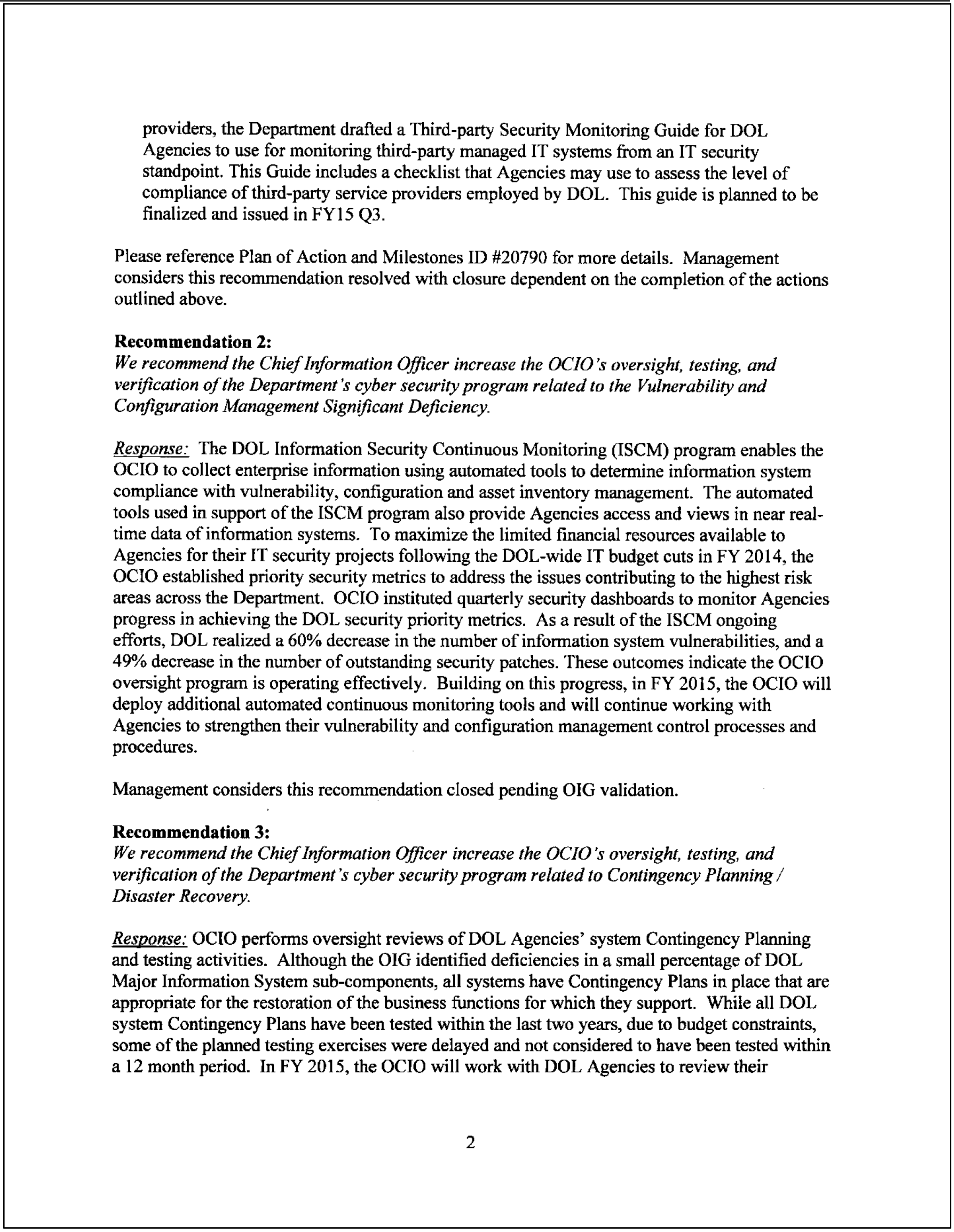
SUBJECT: Management Response to the Office of the Inspector General Fiscal Year 2015 Draft Audit Report Entitled: Cyber Security Program Improvements Are Needed to Better Secure DOL's Major Information Systems, Report No. 23-15-001-07-725

This memorandum responds to the above-referenced Fiscal Year 2015 draft audit report dated March 18, 2015. The Office of Inspector (OIG) performed audit testing of 15 Department of Labor (DOL) major information systems and issued 75 Statements of Facts to the System Owners. As a result of combining the system specific deficiencies, the OIG outlined four DOL entity-wide "significant deficiencies" for Third-Party Oversight/Monitoring, Vulnerability and Configuration Management, Contingency Planning/Disaster Recovery and Access Management resulting in the issuance of four recommendations. Although not considered significant deficiencies, the OIG also identified other Information Technology (IT) security deficiencies for IT Asset Management and Incident Response resulting in the issuance of one recommendation.

The Office of the Chief Information Officer (OCIO) appreciates the efforts of the OIG, and takes very seriously its responsibility to safeguard DOL IT systems and information. Management agrees that improvements are needed to better secure DOL's major information systems and will ensure corrective actions are taken as appropriate. In management's view, the items outlined in the report as contributing to the significant deficiency for Contingency Planning does not provide the requisite linkage between the findings and risks outlined in the report that could realistically be expected to rise to the level of significance at a Department-level. Management's response to the recommendation outlined in the report follows.

Recommendation 1
We recommend the Chief Information Officer establish third-party oversight/monitoring processes and tools that guide information system owners on how to better monitor third-party service providers' effectiveness in implementing NIST information security requirements and Administration priorities.

- <u>*Response:*</u> The DOL Computer Security Handbook, Volume 15, section 3.2.5, establishes the requirements for monitoring third-party compliance with the Department's system security policies and standards. In an effort to strengthen its ability to monitor third-party



providers, the Department drafted a Third-party Security Monitoring Guide for DOL Agencies to use for monitoring third-party managed IT systems from an IT security standpoint. This Guide includes a checklist that Agencies may use to assess the level of compliance of third-party service providers employed by DOL. This guide is planned to be finalized and issued in FY15 Q3.

Please reference Plan of Action and Milestones ID #20790 for more details. Management considers this recommendation resolved with closure dependent on the completion of the actions outlined above.

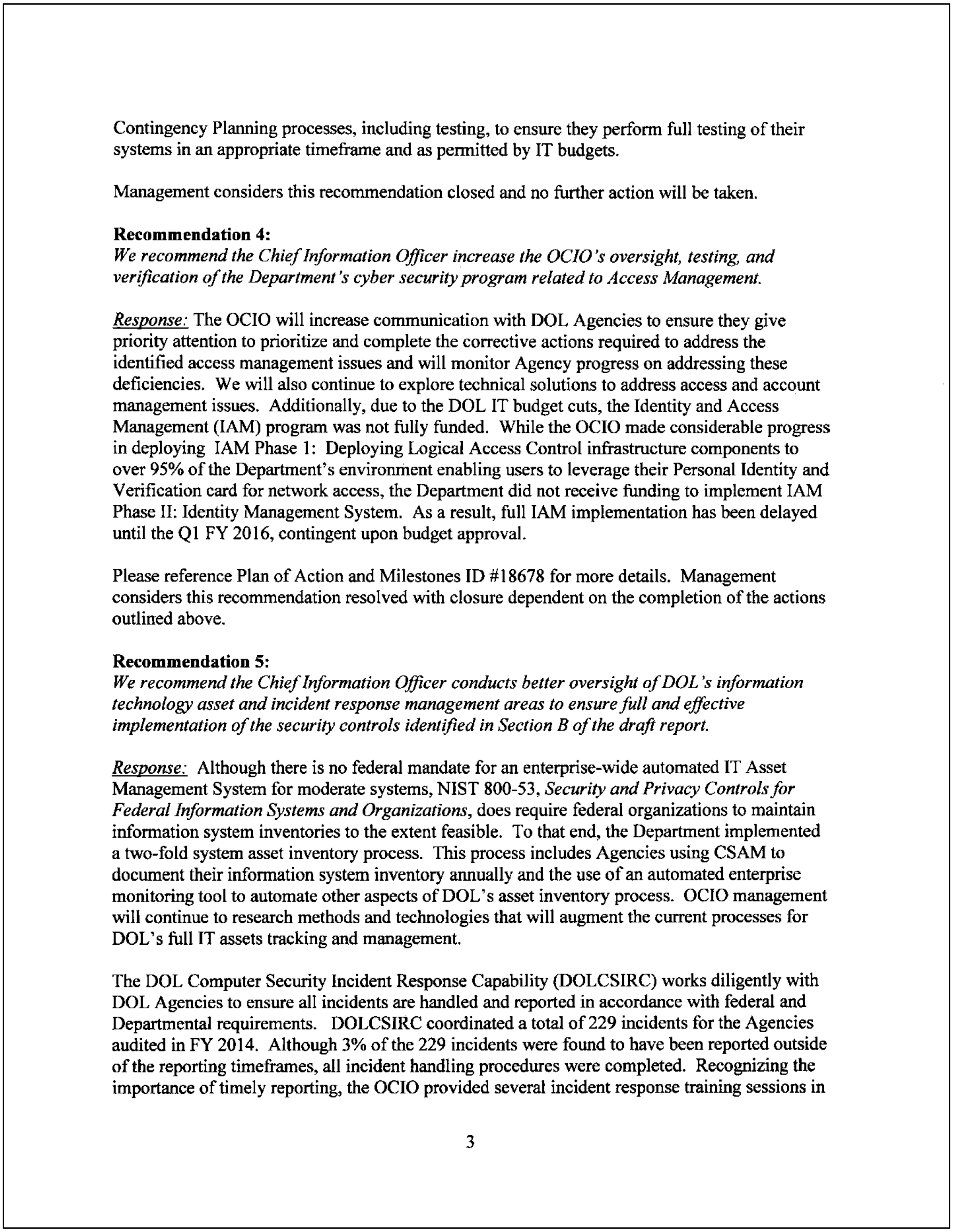
Recommendation 2:
We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of the Department's cyber security program related to the Vulnerability and Configuration Management Significant Deficiency.

Response: The DOL Information Security Continuous Monitoring (ISCM) program enables the OCIO to collect enterprise information using automated tools to determine information system compliance with vulnerability, configuration and asset inventory management. The automated tools used in support of the ISCM program also provide Agencies access and views in near real-time data of information systems. To maximize the limited financial resources available to Agencies for their IT security projects following the DOL-wide IT budget cuts in FY 2014, the OCIO established priority security metrics to address the issues contributing to the highest risk areas across the Department. OCIO instituted quarterly security dashboards to monitor Agencies progress in achieving the DOL security priority metrics. As a result of the ISCM ongoing efforts, DOL realized a 60% decrease in the number of information system vulnerabilities, and a 49% decrease in the number of outstanding security patches. These outcomes indicate the OCIO oversight program is operating effectively. Building on this progress, in FY 2015, the OCIO will deploy additional automated continuous monitoring tools and will continue working with Agencies to strengthen their vulnerability and configuration management control processes and procedures.

Management considers this recommendation closed pending OIG validation.

Recommendation 3:
We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of the Department's cyber security program related to Contingency Planning / Disaster Recovery.

Response: OCIO performs oversight reviews of DOL Agencies' system Contingency Planning and testing activities. Although the OIG identified deficiencies in a small percentage of DOL Major Information System sub-components, all systems have Contingency Plans in place that are appropriate for the restoration of the business functions for which they support. While all DOL system Contingency Plans have been tested within the last two years, due to budget constraints, some of the planned testing exercises were delayed and not considered to have been tested within a 12 month period. In FY 2015, the OCIO will work with DOL Agencies to review their



Contingency Planning processes, including testing, to ensure they perform full testing of their systems in an appropriate timeframe and as permitted by IT budgets.

Management considers this recommendation closed and no further action will be taken.

Recommendation 4:
We recommend the Chief Information Officer increase the OCIO's oversight, testing, and verification of the Department's cyber security program related to Access Management.

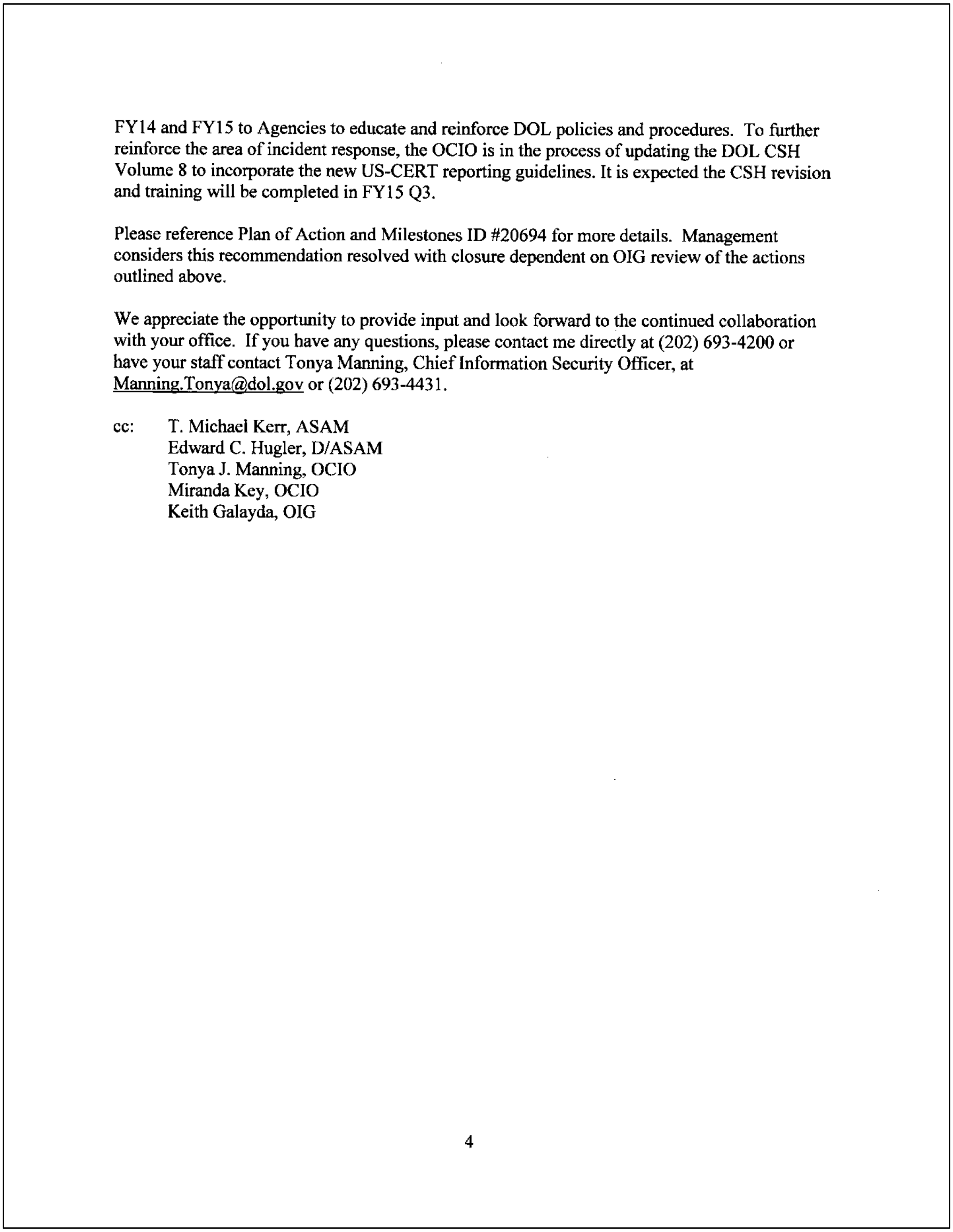
Response: The OCIO will increase communication with DOL Agencies to ensure they give priority attention to prioritize and complete the corrective actions required to address the identified access management issues and will monitor Agency progress on addressing these deficiencies. We will also continue to explore technical solutions to address access and account management issues. Additionally, due to the DOL IT budget cuts, the Identity and Access Management (IAM) program was not fully funded. While the OCIO made considerable progress in deploying IAM Phase 1: Deploying Logical Access Control infrastructure components to over 95% of the Department's environment enabling users to leverage their Personal Identity and Verification card for network access, the Department did not receive funding to implement IAM Phase II: Identity Management System. As a result, full IAM implementation has been delayed until the Q1 FY 2016, contingent upon budget approval.

Please reference Plan of Action and Milestones ID #18678 for more details. Management considers this recommendation resolved with closure dependent on the completion of the actions outlined above.

Recommendation 5:
We recommend the Chief Information Officer conducts better oversight of DOL's information technology asset and incident response management areas to ensure full and effective implementation of the security controls identified in Section B of the draft report.

Response: Although there is no federal mandate for an enterprise-wide automated IT Asset Management System for moderate systems, NIST 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, does require federal organizations to maintain information system inventories to the extent feasible. To that end, the Department implemented a two-fold system asset inventory process. This process includes Agencies using CSAM to document their information system inventory annually and the use of an automated enterprise monitoring tool to automate other aspects of DOL's asset inventory process. OCIO management will continue to research methods and technologies that will augment the current processes for DOL's full IT assets tracking and management.

The DOL Computer Security Incident Response Capability (DOLCSIRC) works diligently with DOL Agencies to ensure all incidents are handled and reported in accordance with federal and Departmental requirements. DOLCSIRC coordinated a total of 229 incidents for the Agencies audited in FY 2014. Although 3% of the 229 incidents were found to have been reported outside of the reporting timeframes, all incident handling procedures were completed. Recognizing the importance of timely reporting, the OCIO provided several incident response training sessions in



FY14 and FY15 to Agencies to educate and reinforce DOL policies and procedures. To further reinforce the area of incident response, the OCIO is in the process of updating the DOL CSH Volume 8 to incorporate the new US-CERT reporting guidelines. It is expected the CSH revision and training will be completed in FY15 Q3.

Please reference Plan of Action and Milestones ID #20694 for more details. Management considers this recommendation resolved with closure dependent on OIG review of the actions outlined above.

We appreciate the opportunity to provide input and look forward to the continued collaboration with your office. If you have any questions, please contact me directly at (202) 693-4200 or have your staff contact Tonya Manning, Chief Information Security Officer, at Manning.Tonya@dol.gov or (202) 693-4431.

cc: T. Michael Kerr, ASAM
Edward C. Hugler, D/ASAM
Tonya J. Manning, OCIO
Miranda Key, OCIO
Keith Galayda, OIG

TO REPORT FRAUD, WASTE OR ABUSE, PLEASE CONTACT:

Online:	http://www.oig.dol.gov/hotlineform.htm
Email:	hotline@oig.dol.gov
Telephone:	1-800-347-3756 202-693-6999
Fax:	202-693-7020

Address: Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue, N.W.
Room S-5506
Washington, D.C. 20210