

# U.S. Department of Labor

Office of Inspector General—Office of Audit

**REPORT TO THE CHIEF  
INFORMATION OFFICER**



**FISMA FISCAL YEAR 2015:  
ONGOING SECURITY  
DEFICIENCIES EXIST**

**Date Issued: November 30, 2016**  
**Report Number: 23-16-002-07-725P**

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

## **BRIEFLY...**

**September 30, 2016**

### **FISMA FISCAL YEAR 2015: ONGOING SECURITY DEFICIENCIES EXIST**

#### **WHY OIG CONDUCTED THE EVALUATION**

Congress, the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Government Accountability Office (GAO) 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 Modernization Act (FISMA) in 2002, and revised it in 2014. FISMA requires all executive agencies to use standards put forth by the National Institute of Standards and Technology (NIST) to protect their information and information systems.

Under FISMA, federal agencies are required to independently evaluate their information security programs and practices every year.

#### **WHAT OIG DID**

We conducted an evaluation to determine the following:

Did DOL implement effective FISMA minimum information security requirements?

For FY 2015, we tested 15 nonfinancial systems (10 DOL agency systems and 5 contractor systems) and 8 financial systems (5 DOL systems and 3 contractor systems), using Office of Management and Budget/Department of Homeland Security metrics, National Institute of Standards and Technology guidance, and DOL policies and procedures.

#### **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/2016/23-16-002-07-725P.pdf>

#### **WHAT OIG FOUND**

DOL controls had not been fully implemented or were not operating effectively to meet minimum FISMA security requirements. Our testing of selected controls identified 116 deficiencies across 8 of the 10 FISMA security areas. Of those 116 deficiencies, 60 were related to identity and access management, a key control area for ensuring an authenticated user accesses only what they are authorized to access and no more. Numerous deficiencies were also identified in the areas of contingency planning (20) and configuration management (17).

Despite many previous reports that identified similar control weaknesses, these deficiencies continue to exist or reoccur, and represent ongoing, unnecessary risks to the confidentiality, integrity, and availability of DOL's information. The deficiencies identified in this report occurred because the internal control framework in the eight FISMA control areas has not been effective. The ineffectiveness of the internal control framework was due, in part, to the CIO not having the independence and authority at the department level for implementing and maintaining an effective information security program.

#### **WHAT OIG RECOMMENDED**

We recommended the Assistant Secretary for Administration and Management realign the organizational structure as it relates to the CIO to address the organizational independence issue identified in this report. Additionally, we recommended the CIO work with Program Agency management to develop corrective actions for the deficiencies identified in this report.

The CIO generally agreed to the findings in the report, but indicated further linkage to risks would have been beneficial. The CIO stated a corrective action program has been implemented to address the reported and other information security deficiencies. The CIO disagreed with the OIG's recommendation to realign the organizational structure to address the CIO independence issue. She asserted the CIO reporting arrangement is defined in a way that best works for DOL and is aligned with the Office of Management and Budget's Federal Information and Technology Acquisition Reform Act CIO assignment plan.

**TABLE OF CONTENTS**

**INSPECTOR GENERAL'S REPORT** ..... 1

**RESULTS IN BRIEF** ..... 2

**BACKGROUND** ..... 2

**RESULTS** ..... 3

    1) Identity and Access Management ..... 5

    2) Contractor Systems..... 8

    3) Configuration Management ..... 8

    4) Contingency Planning ..... 8

    5) Incident Response and Reporting ..... 10

    6) Plan of Action & Milestones..... 11

    7) Risk Management ..... 11

    8) Continuous Monitoring ..... 12

**RECOMMENDATIONS**..... 14

**EXHIBIT**

    (A) ISCM Maturity Model Definitions..... 17

**APPENDICES**

    (A) Objective, Scope, Methodology, and Criteria..... 22

    (B) Management Response..... 26

    (C) Acronyms..... 28

    (D) Acknowledgements ..... 29

**U.S. Department of Labor**

Office of Inspector General  
Washington, D.C. 20210



September 30, 2016

## **INSPECTOR GENERAL'S REPORT**

Dawn M. Leaf  
Chief Information Officer  
200 Constitution Avenue, NW  
Washington, DC 20210

Congress, the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and the Government Accountability Office (GAO) 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 Modernization Act (FISMA) in 2002, and revised it in 2014. FISMA requires all executive agencies use National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 200 and Special Publication (SP) 800-53, Revision 4, 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.

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.

We performed an evaluation to determine:

Did DOL implement effective FISMA minimum information security requirements?

Using the Office of Management and Budget / Department of Homeland Security metrics, National Institute of Standards and Technology guidance, and DOL policies and procedures, we tested 23 systems in Fiscal Year (FY) 2015. This included 15 nonfinancial and 8 financial systems. For the nonfinancial systems, there were 10 DOL agency systems and 5 contractor systems. For the 8 financial systems, there were 5 DOL systems and 3 contractor systems.

## RESULTS IN BRIEF

DOL controls had not been fully implemented or were not operating effectively to meet minimum FISMA security requirements for the selected systems and security control areas we tested. Our testing of selected controls identified 116 deficiencies across 8 of the 10 FISMA security areas.<sup>1</sup> Of those 116 deficiencies, 60 were related to identity and access management, a key control area for ensuring an authenticated user accesses only what they are authorized to access and no more. Numerous deficiencies were also identified in the areas of contingency planning (20) and configuration management (17).

Despite many previous reports that identified similar control weaknesses, these deficiencies, some of which were first identified in 2005, continue to exist or reoccur, and represent ongoing, unnecessary risks to the confidentiality, integrity, and availability of DOL's information. DOL's inability to correct these deficiencies stems, in part, from a governance structure that does not provide the CIO with the independence needed to carry out the responsibilities of the position.

## 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 Federal Information Security Modernization Act of 2014 was passed on December 12, 2014, and changes require information security programs to use a continuous monitoring process, rather than the formerly used cyclical checklist approach to assist in improving the effectiveness of the security program.

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.

---

<sup>1</sup> The 10 FISMA security areas are continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems.

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] 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.

Section 811 of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for FY 2015 amends the Clinger-Cohen Act by providing explicit accountability to the CIO to: manage all information technology resources, including approving the information technology portion of the annual budget requests submitted to Congress; approve all information technology and information technology service contracts; and approve the appointment of any component-level Chief Information Officer.

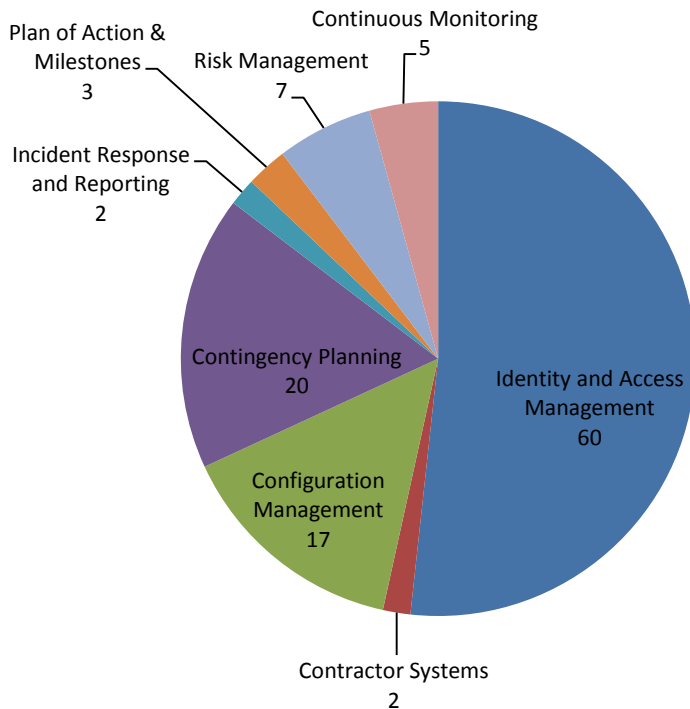
## **RESULTS**

For the selected systems and security controls tested, we identified 116 individual deficiencies in the following 8 security control areas:

- 1) Identity and Access Management
- 2) Contractor Systems
- 3) Configuration Management
- 4) Contingency Planning
- 5) Incident Response and Reporting
- 6) Plan of Action & Milestones
- 7) Risk Management
- 8) Continuous Monitoring

The following chart shows the breakdown of the deficiencies identified within FISMA security control areas.

**FISMA Security Control Area Deficiencies**



Management, which is charged with oversight and accountability for the DOL information technology (IT) control environment, had not remediated the widespread deficiencies in multiple information systems, some of which were first identified in 2005. This lack of management oversight and accountability for the DOL IT control environment has resulted in ongoing unnecessary risks to the confidentiality, integrity, and availability of DOL’s information.

Despite many previous reports that have repeatedly identified similar control weaknesses, the deficiencies have not been corrected. The Department’s inability to correct these deficiencies stems, in part, from a governance structure that does not provide the CIO with the independence needed to carry out the responsibilities of the position. *Standards for Internal Control in the Federal Government*, as prescribed by the Comptroller General of the United States, states:

Management establishes the organizational structure necessary to enable the entity to plan, execute, control and assess the organization in achieving its objectives. Management develops the overall responsibilities from the entity’s

objectives that enable the entity to achieve its objectives and address related risks.

An organizational structure that provides the CIO with the necessary authority and independence is crucial because the CIO is required to carry out departmental responsibilities under the Clinger-Cohen Act, Computer Security Act of 2015, FISMA 2014, and FITARA 2013. FITARA 2013 requires assurance that approximately \$500 million annually is directed toward ongoing and future IT investments and projects, including information security. With the CIO positioned in the Office of the Assistant Secretary of Administration and Management (OASAM), a major user and architect of DOL's information technology that also has a substantial influence over budgetary and procurement matters, the CIO may not have the independence needed to carry out his or her responsibilities and meet departmental objectives.

---

## **IDENTITY AND ACCESS MANAGEMENT**

---

Consistent with findings reported over the past ten years, in FY 2015, we identified pervasive deficiencies in the area of Identity and Access Management. Access Management, Identification and Authentication, and Audit and Accountability controls were not operating as intended to detect and prevent unauthorized and unnecessary access to entity-wide processes in 13 of the 23 systems tested. Our testing revealed 48 Access Management deficiencies, 4 Identification and Authentication deficiencies, and 8 Audit and Accountability deficiencies.

### **ACCESS MANAGEMENT DEFICIENCIES**

Thirteen of the 23 systems tested, including entity-wide tests, revealed 48 Access Management deficiencies related to Access Control Policy, Account Management, Separation of Duties, Least Privilege, Remote Access, Personnel Separation, Security Awareness and Role Based Training, Personnel Authorization, Rules of Behavior, and Access Agreements Security Controls.

#### *ACCOUNT MANAGEMENT TESTING REVEALED USER ACCOUNTS ACTIVE AFTER USER TERMINATION*

Ten of the 23 systems tested still had active user accounts after users had been terminated, while four systems had user accounts that could be accessed after users had been terminated. Removing access to user accounts as soon as individuals are terminated eliminates the risk of unauthorized access. Instead, accounts for these terminated users were either currently active as of testing or had been active for a period of time after the users' termination dates.

In addition, 6 of 23 systems tested had not disabled user accounts after 60 days of inactivity as required by the DOL Computer Security Handbook. These inactive accounts were



vulnerable to unauthorized access to information contained on any system available to the inactive user.

*SYSTEMS LACKED SEPARATION OF DUTIES*

We determined 5 of 23 systems tested lacked appropriate separation of duties. For example, one system had no separation of duties (SOD) matrix to identify and define business function roles. In addition, a user had both system and database administrator access from October 1, 2014, until June 24, 2015. The Authorizing Official, the Office of Chief Information Officer, and the Chief Information System Officer had accepted the risk that an individual would have both system and database administrator access by completing the Segregation of Duties CSH Policy/Procedure Exemption Request Form. However, in another system, three users had both system and database administrator access, a risk that DOL had not formally accepted. This type of access would allow users to remove and delete data and also conceal their actions.

We also determined two of the systems tested did not enforce separation of duties based on a SOD matrix. For one of the systems, 10 out of 85 users had conflicting roles and for the other, 5 out of 2,066 users had conflicting roles. This would allow users to both initiate and approve transactions that, for example, would impact salary or awards to employees. In addition, we determined for another system a developer had access to the production environment, which could have allowed the developer to make changes that could bypass the configuration / change management process.

Such deficiencies unacceptably raise the risk of individuals being afforded unchecked opportunities for abuse, including, but not limited to, introducing fraudulent data or malicious code into the system.

*SYSTEMS DID NOT FOLLOW RULES OF BEHAVIOR /  
ACCESS AGREEMENTS TESTING*

Three of 23 systems tested did not ensure all required documents were completed prior to individuals being granted access as required by the DOL Computer Security Handbook. Further, Rules of Behavior did not restrict the use of social media and networking sites as required by NIST SP 800-53 Revision 4, Control PL-4 for System 9, 1, and 3. Without proper Access Management controls, unauthorized or authorized individuals could execute inappropriate transactions in the affected DOL systems.

In response to this deficiency, Rules of Behavior for two systems were updated on September 29, 2015, and September 30, 2015, respectively, to include explicit restrictions on the use of social media and networking sites. Additionally, OASAM management created a Plan of Action & Milestones (POA&M) with completion dates in FY 2016.

## **IDENTIFICATION AND AUTHENTICATION NOT ENSURED**

Three of 23 systems tested did not ensure Identification and Authentication, Authenticator Management controls regarding generic/shared accounts, password settings, Personal Identity Verification (PIV), and Session Locks. The minimum baseline controls for Identification and Authentication and Authenticator Management are designed to make all user accounts accountable to an individual or process, verify who accesses the system, and provide assurance of user identity.

### *MOST GENERIC ACTIVE ACCOUNTS FOR ONE SYSTEM WERE PROHIBITED BY DOL POLICY*

Sixty-one of 78 generic active accounts for one system we tested were prohibited by DOL policy. DOL policy requires unique, as opposed to generic, user accounts so an individual user can be identified and held accountable for any actions taken from that account or process. When prohibited generic accounts were used to process grant transactions, it would not be possible to determine the identity of the processors or review which individual had processed specific grant transactions. As a result, Program Agency management would not be able to determine accountability for specific actions.

### *PASSWORD CONFIGURATION SETTINGS DEFICIENCIES*

Two of the 23 systems tested had password configuration setting deficiencies in the control that established parameters (i.e., password composition, length, life, history) that the system used to identify who has access to the system. These password settings ensure that requirements can be enforced (such as changing passwords every so often) to make it very difficult to gain access by guessing another user's password. The application, database, and operating system password configurations were not configured in accordance with the DOL CSH.

When user account security was not configured in accordance with the DOL CSH, individuals could access system data.

### *PERSONAL IDENTITY VERIFICATION NOT IMPLEMENTED*

During FY 2015, OASAM management informed us that DOL had fully implemented PIV for logical access. However, the PIV cards were not implemented until July 15, 2015, in response to an OMB mandate. Further, OASAM could not provide a PIV implementation plan to show PIV cards had been fully implemented across the organization. This has been a longstanding issue. As a result of the OMB CyberSecurity Sprint, OASAM did implement PIV usage for privileged users, but end users were still being implemented and OASAM had a planned completion date of December 31, 2015.

## **AUDIT AND ACCOUNTABILITY CONTROL DEFICIENCIES**

Six of the 23 systems tested had Audit and Accountability control deficiencies. The six systems did not document their audit log reviews. Also, for one of the systems tested, the

log aggregate tool was operational, but not used because of a related expired software license. Without the ability to gather or review audit logs, systems were at an increased level of risk of fraudulent activities that might compromise data. Without proper and timely review of audit logs, unauthorized access or activity could not be identified.

---

## **CONTRACTOR SYSTEMS**

---

For 7 of 8 contractor systems tested, system owners were not monitoring third party providers' compliance with DOL security requirements. As a result, it could not be determined if security controls operated as intended for the third-party service providers. This occurred because DOL had not fully implemented policies and procedures that ensure monitoring of system owner requirements.

These deficiencies have reoccurred for the past two years and demonstrate the OCIO had not effectively implemented controls related to the Third-Party Oversight / Monitoring.

Not providing guidance to designated personnel and monitoring the oversight of these third-party systems makes it very likely the system's security posture would not be consistently reported to the authorizing officials and DOL would not know if the third party systems were complying with mandatory security requirements.

---

## **CONFIGURATION MANAGEMENT**

---

Seven of 23 information systems were not operating as intended in the areas of information integrity and configuration management. We identified 17 total deficiencies within the Information Integrity (7) and Configuration Management (10) security control areas.

Strong Vulnerability Flaw Remediation and Configuration Management control practices reduce the risk of system exposure to known deficiencies, malicious technical attacks, and unauthorized or unintentional changes. DOL did not consistently follow policies and procedures identified in the CSH for implementing patches and changes that correct security weaknesses and application changes. Program agencies had taken corrective actions for some of the deficiencies noted above to mitigate the system-level deficiencies, such as the CyberSecurity Sprint that was mandated by OMB that included implementing outstanding patches for operating systems. OCIO's efforts to reduce the number of these deficiencies were not sufficient to achieve acceptable risk since these deficiencies were across multiple systems.

---

## **CONTINGENCY PLANNING**

---

Six of 23 information systems tested for contingency planning were not operating as intended. These deficiencies included: 1) developing a contingency plan, 2) testing the contingency plan, 3) identifying alternate processing sites, and 4) ensuring information system backup and information system recovery and reconstitution. The testing identified

incomplete contingency planning, incorrect or out-of-date contingency plans, untested system backups, and insufficient contingency plan testing.

Effective planning and prioritization of essential systems and processes enables organizations to recover and operate without excessive interruptions. Furthermore, testing the contingency plan is vital to determine its effectiveness and locate deficiencies in the plan. Identifying deficiencies and training relevant staff must precede activating the plan in the event of a disaster or information system compromise.

**CONTINGENCY PLAN DEVELOPMENT LACKED  
COORDINATION AMONG SYSTEM OWNERS**

Testing revealed a lack of coordination and communication among system owners and OASAM (the hosting organization) for contingency planning activities. While in the process of consolidating servers that support these applications, OASAM did not coordinate efforts among system owners to the level required by the DOL CSH, which requires coordination among the groups responsible for contingency planning.

The lack of a contingency plan that integrates all groups responsible for the application and support system increases the risk to timely recovery of the system.

**CONTINGENCY PLAN NOT COMPREHENSIVELY  
TESTED/CONTAINED INCORRECT INFORMATION**

Two of 23 systems performed only limited testing of the contingency plans and/or had incorrect or outdated information in the management-approved plan. The testing of contingency plans was limited to tabletop exercises and was not comprehensive. Management for one system stated to OIG that its contingency plan test efforts for FY 2015 were deferred because of the change of key DOL personnel and competition with other security-related tasks. Management for the other of the two systems offered no explanation as to why no testing was performed during the year. Without testing of the contingency plan, agency personnel cannot be prepared to handle contingency plan procedures in the event of a crisis.

**ALTERNATE PROCESSING SITES NOT IDENTIFIED**

Seven of 23 systems did not have an alternate processing site identified in the contingency plan as required. The inability to identify an alternate processing site for moderate risk systems would mean that systems would not meet their Recovery Time Objective (RTO) and availability requirements. This, in turn, would mean DOL would not be able to fulfill its essential business missions and functions.

**NO EVIDENCE INFORMATION SYSTEM BACKUP PERFORMED ACCORDING TO POLICY**

Ten of 23 systems tested did not provide evidence that backups were performed according to policy. Without performing information system backups in a timely manner, DOL

increased the risk that data residing within the information systems would not be restored in the event of data corruption or loss.

---

## **INCIDENT RESPONSE AND REPORTING**

---

We inspected a random selection of 25 incidents and determined 5 were not reported to the DOL Computer Security Incident Response Center (CSIRC) and subsequently to the United States Computer Emergency Readiness Team (US-CERT) within the timeframe required by the DOL Computer Security Handbook and US-CERT for entity-wide and System 1 controls tested.

Specifically, we identified the following:

- A category-4 incident was reported to US-CERT<sup>2</sup> approximately 4 months after the event occurred, instead of the required time of 1 week.
- 3 entity-wide, category-1 incidents selected for testing were not reported to DOL's CSIRC within the DOL Computer Security Handbook required timeframe.
- OASAM did not complete POA&M's 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 conducted tests to ascertain the severity of the incident; however, the initial incident form identified a potential disclosure of a confidential survey participant's personal information. This should have signaled a category-1 incident and been reported to US-CERT within one hour.

Because cyber attacks compromise data, quick response is essential when security breaches occur. Without having developed and implemented a coordinated approach to respond to such incidents, DOL agencies risked loss or theft of information, including personal and private student information, and disruption of services.

Failure to report incidents within the designated timeframe can result in an untimely response to critical incidents and delay the incident correlating capability of DOL, which can potentially leave DOL and its agencies vulnerable to further unauthorized access or attacks.

---

<sup>2</sup> US CERT defines Categories 0 through 6 (CAT 0 – 6) on their website at <https://www.us-cert.gov/government-users/reporting-requirements>

---

## **PLAN OF ACTION AND MILESTONES**

---

Review and monitoring of POA&Ms were not performed timely (within 45 days after the end of the quarter) for 9 information systems and updates to the POA&Ms were not completed. Specifically:

- Quarter (Q) 1 POA&Ms were not submitted to the system timely, ranging from 90 to 119 days after the end of Q1;
- No Q3 or Q4 POA&Ms were submitted as of October 1, 2015;
- No POA&Ms were submitted for the entire FY 2015 as of October 1, 2015;
- As of May 26, 2015, 2 of 12 POA&M items were not closed timely; and
- Twenty-four POA&M items did not have start dates and 20 of the items were delayed with no reason provided.

Program Agency system management stated there was a lack of management oversight and communication in providing information to OASAM and updating POA&M information.

Failure to timely inform agencies of the results of the POA&M review and failure to ensure completeness and accuracy of agencies' POA&Ms and remediation actions unnecessarily places DOL systems at risk. Agencies may not be taking steps to remediate identified weaknesses, which could affect the confidentiality, integrity, and availability of information system data.

---

## **RISK MANAGEMENT**

---

Five of 23 DOL information systems had implemented controls based on NIST Special Publication (SP) 800-53, Revision 3, but they should have followed Revision 4.

Additionally, no evidence could be provided that one system owner had analyzed the status of security controls designated as: (1) inherited from another system, or (2) not-applicable during their most recent Security Controls Assessment (SCA). Of the 274 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 controls in scope, 125 were listed as Inherited or Not Applicable, and therefore were not analyzed as part of the SCA.

Finally, there were multiple agencies migrating their system and management controls platforms into another system. The ongoing reorganization process led to confusion on the part of both systems staff, which led to the environment lacking proper oversight and communication. This resulted in the controls required by NIST 800-53 not being implemented by either party.

The system owner contends specific guidance does not exist, indicating a required timeframe for re-authorization documentation of systems to be completed following leadership turnover. As a result, the system owner completed re-authorization documentation after the position was permanently filled for the AO.

DOL lacks specific guidance in regard to inherited controls being included in a system's SCA. As a result, the assessor did not document the analysis performed on the specific controls that were designated previously as inherited or not-applicable to determine if these classifications were still valid.

Failing to document an up-to-date system security plans and certification and accreditation documentation may have a negative effect on subsequent security activities. Specifically, the system owners may not be able to implement, assess, authorize, and monitor the security controls properly for the selected systems. Therefore, the system security controls may not be sufficient to protect the confidentiality, integrity, and availability of sensitive information.

---

## **CONTINUOUS MONITORING**

---

In FY15, DHS and OMB asked the OIG to assess the Department's continuous monitoring process based on a five-scale maturity model evaluating the people, processes, and technology within the department as it pertains to information security continuous monitoring. The five levels specified in Exhibit A include:

- Level 1: Ad-hoc
- Level 2: Defined
- Level 3: Consistently Implemented
- Level 4: Managed and Measurable
- Level 5: Optimized

DOL has defined the stakeholders of the ISCM program, identified which skills are needed and the gaps that currently exist for individuals that support the ISCM program, shared ISCM information with individuals with significant security responsibilities, and tied DOL ISCM activities to DOL's Enterprise Risk Management Strategy (ERMS).

However, DOL had gaps in the ISCM program processes. Specifically, DOL had not:

- implemented controls or tools to address ongoing assessments and monitoring of security controls;
- performed hardware asset management, software asset management, configuration setting management, or common vulnerability management;
- collected security related information required for metrics, assessments, and reporting;
- analyzed ISCM data and report findings; or
- determined the appropriate risk responses.

Additionally, DOL has not defined qualitative and quantitative performance measures that would allow it to share information among stakeholders. We noted DOL started a process to identify, procure, and deploy tools to build-up the ISCM program.

- - - - -

The deficiencies identified in this report occurred because the internal control framework in the eight areas discussed above has not been effective. The ineffectiveness of the internal control framework was due, in part, to the CIO not having the independence and authority at the department level for implementing and maintaining an effective information security program.

*Standards for Internal Control in the Federal Government*, as prescribed by the Comptroller General of the United States, states:

Management establishes the organizational structure necessary to enable the entity to plan, execute, control and assess the organization in achieving its objectives. Management develops the overall responsibilities from the entity's objectives that enable the entity to achieve its objectives and address related risks.

Management develops and organizational structure with an understanding of the overall responsibilities to discrete units to enable the organization to operate in an efficient and effective manner, comply with applicable laws and regulations, and reliable report quality information. Based on the nature of assigned responsibility, management chooses the type and number of discrete units, such as divisions, offices, and related subunits.

As part of establishing an organizational structure, management considers how units interact in order to fulfill their overall responsibilities. Management establishes reporting lines within the organizational structure so that units can communicate the quality of information necessary for each unit to fulfill its overall responsibilities. Reporting lines are defined at all levels of the organization and provide methods of communication that can flow down, across, up, and around the structure. Management also considers the entity's overall responsibilities to external stakeholders and established reporting lines that allow the entity to both communicate and receive information from external stakeholders.

Additionally, an ad-hoc<sup>3</sup> continuous monitoring program has not identified information security control weaknesses across all systems. As a result, these weaknesses continue to exist or reoccur repeatedly.

---

<sup>3</sup> Ad-hoc as defined by the FY 2015 OIG FISMA metrics - program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137.



DOL's continuous monitoring management program was assessed as an ad-hoc program (level 1), the very lowest score possible. In contrast, level 5 maturity means programs are managed and measurable, the organization's information security continuous monitoring program is institutionalized, repeatable, self-regenerating, and is updated in a near real-time basis in reaction to changes in business/mission requirements and a changing threat and technology landscape.

## OIG'S RECOMMENDATIONS

We recommend the Assistant Secretary of the Office of Administration and Management:

1. Realign the organizational structure as it relates to the CIO to address the organizational independence issue identified in this report.

Additionally, we recommend the OCIO:

2. Work with Program Agency management to develop and track corrective action progress for identified deficiencies.

---

## MANAGEMENT RESPONSE

---

The CIO generally agreed that several of the individual instances cited in the report are accurate, but suggested that findings cited are not consistent with DOL's current security posture, which she stated has been consistently improving since 2015. The CIO also generally agreed with the findings in the report, but indicated further linkage to risks would have been beneficial. The CIO indicated DOL is committed to ensuring the security of its information and information systems and will continue its efforts to ensure corrective action plans are developed and implemented to address the identified deficiencies. Further, the CIO stated a corrective action program has been developed to address the deficiencies in this report as well as other deficiencies.

The CIO disagreed with the OIG's recommendation to realign the organizational structure to address the CIO independence issue. She asserted the CIO reporting arrangement is defined in a way that best works for DOL and is aligned with the Office of Management and Budget's Federal Information Technology Acquisition Reform Act CIO assignment plan.

Management's response to our draft report is included in its entirety in Appendix B.

We appreciate the cooperation and courtesies OCIO and other DOL agency personnel extended to the Office of Inspector General during this audit. OIG personnel who made major contributions to this report are listed in Appendix D.



Elliot P. Lewis  
Assistant Inspector General  
for Audit

## Exhibit

---

**Exhibit A: ISCM Maturity Model Definitions**

Level	Definition
<p>1 Ad-hoc</p>	<p>ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.</p> <ul style="list-style-type: none"> <li>• ISCM activities are performed without the establishment of comprehensive policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.</li> <li>• ISCM stakeholders and their responsibilities have not been defined and communicated across the organization.</li> <li>• ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used.</li> <li>• The organization lacks personnel with adequate skills and knowledge to effectively perform ISCM activities.</li> <li>• The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk.</li> <li>• The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management.</li> <li>• ISCM activities are not integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements.</li> <li>• There is no defined process for collecting and considering lessons learned to improve ISCM processes.</li> <li>• The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.</li> </ul>
<p>2 Defined</p>	<p>The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.</p> <ul style="list-style-type: none"> <li>• ISCM activities are defined and formalized through the establishment of comprehensive ISCM policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137,</li> </ul>

	<p>OMB M-14-03, and the CIO ISCM CONOPS.</p> <ul style="list-style-type: none"> <li>• ISCM stakeholders and their responsibilities have been defined and communicated across the organization, but stakeholders may not have adequate resources (people, processes, tools) to consistently implement ISCM activities.</li> <li>• ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used.</li> <li>• The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization.</li> <li>• The organization has identified and fully defined the ISCM technologies it plans to utilize in the ISCM automation areas. Automated tools are implemented to support some ISCM activities but the tools may not be interoperable. In addition, the organization continues to rely on manual/procedural methods in instances where automation would be more effective.</li> <li>• The organization has defined how ISCM activities will be integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. However, the organization does not consistently integrate its ISCM and risk management activities.</li> <li>• The organization has defined its process for collecting and considering lessons learned to make improvements to its ISCM program. Lessons learned are captured but are not shared at an organizational level to make timely improvements.</li> <li>• ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions.</li> </ul>
<p>3 Consistently Implemented</p>	<p>In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.</p> <ul style="list-style-type: none"> <li>• The ISCM program is consistently implemented across the organization, in accordance with the organization’s ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS.</li> <li>• ISCM stakeholders have adequate resources (people, processes, technologies) to effectively accomplish their duties.</li> <li>• The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization.</li> <li>• The organization has standardized and consistently implemented its defined technologies in all of the ISCM automation areas. ISCM tools</li> </ul>

	<p>are interoperable, to the extent practicable.</p> <ul style="list-style-type: none"> <li>• ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements.</li> <li>• The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes.</li> <li>• ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations.</li> </ul>
<p>4 Managed and Measurable</p>	<p>In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.</p> <ul style="list-style-type: none"> <li>• Qualitative and quantitative measures on the effectiveness of the ISCM program are collected across the organization and used to assess the ISCM program and make necessary changes.</li> <li>• Data supporting ISCM metrics is obtained accurately, consistently, and in a reproducible format, in accordance with the organization’s ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS.</li> <li>• ISCM data is analyzed consistently and collected and presented using standard calculations, comparisons, and presentations.</li> <li>• ISCM metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities, including situational awareness and risk response.</li> <li>• ISCM metrics provide persistent situational awareness to stakeholders across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations, the organization’s infrastructure, and security domains.</li> <li>• ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&amp;M) up to date on an ongoing basis.</li> </ul>

<p>5 Optimized</p>	<p>In addition to being managed and measurable (Level 4), the organization’s ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.</p> <ul style="list-style-type: none"><li>• Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.</li><li>• The ISCM program is integrated with strategic planning, enterprise architecture and capital planning and investment control processes.</li><li>• The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.</li></ul>
------------------------	---

## Appendices

---



**APPENDIX A**

---

**OBJECTIVE, SCOPE, METHODOLOGY, AND CRITERIA**

---

**OBJECTIVE**

Did DOL implement effective FISMA minimum information security requirements?

**SCOPE**

Using the Office of Management and Budget / Department of Homeland Security metrics, National Institute of Standards and Technology guidance, and DOL policies and procedures we tested in FY 2015 23 systems. This included 15 nonfinancial and 8 financial systems. For the nonfinancial systems there were 10 DOL agency systems and 5 contractor systems. For the 8 financial systems there were 5 DOL systems and 3 contractor systems. We selected a subset of DOL systems and NIST SP 800-53 Revision 4 security control areas using a risk-based approach for testing.

The scope of our testing included the information controls in place during the period of October 1, 2014, through September 30, 2015. We conducted our testing at the Frances Perkins Building in Washington, DC.

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 selected controls in the DOL Cyber Security Program from the following 10 security control areas:

- 1) Continuous monitoring management;
- 2) Configuration management;
- 3) Identity and access management;
- 4) Incident response and reporting;
- 5) Risk management;
- 6) Security training;
- 7) Plan of action and milestones (POA&M);
- 8) Remote access management;
- 9) Contingency planning; and
- 10) Contractor system.

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.

## **METHODOLOGY**

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

### 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 minimum 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.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, and the DHS FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics, dated June 19, 2015.

We mapped the requirements of FY2015 DHS/OMB questions to the NIST SP 800-53, Revision 4 security controls. The goal of the Critical Controls is to strengthen the defensive posture of DOL's information security; reduce compromises, recovery efforts, and associated costs; and protect critical assets and infrastructure. The Controls provide continuous, automated monitoring of the most at risk portions of DOL's information technology infrastructure. Having them in place will allow DOL to focus on its primary mission.

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

To assess the effectiveness of the information security program and practices of the DOL, our scope will include the following:

- Conducting inquiries of information system owners, ISSO, system administrators, and other relevant individuals to walk through each control process.
- An inspection of the information security practices and policies established by the OCIO.
- An inspection of the information security practices, policies, and procedures in use across DOL.

When necessary, we made selections to evaluate specific control elements within the areas of user account forms, terminated users, and configuration management changes in the selected information systems.

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 based on the testing of security controls. The results from testing of the financial systems were also used.

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 evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Quality Standards for Inspection and Evaluation. 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 evaluation objective. We believe that the evidence obtained provides a reasonable basis for our results and conclusions based on our objective.

### **CRITERIA**

We focused our FISMA evaluation approach on federal information security guidance developed by NIST and OMB. NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies' security programs.

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

- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- FISMA of 2002
- FISMA revised 2014
- NIST SP 800-53 Revision 4
- Relevant NIST SP 800 documents
- Department of Labor Manual Series 9 - Information Management
- DOL Computer Security Handbook
- Committee on Sponsoring Organizations on the Treadway Commission

APPENDIX B

**MANAGEMENT’S RESPONSE**


U.S. Department of Labor

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



SEP 30 2016

MEMORANDUM FOR: ELLIOT P. LEWIS  
Assistant Inspector General for Audit

FROM: Dawn Leaf   
Chief Information Officer

SUBJECT: Management Response to the Office of the Inspector General  
Fiscal Year 2015: Ongoing Deficiencies Exist, Report Number:  
23-16-002-07-725

This memorandum responds to the above-referenced draft Fiscal Year 2015 audit report dated September 26, 2016. During the audit period of October 1, 2014 through September 30, 2015, the Office of the Inspector General (OIG) identified deficiencies across eight (8) security controls areas for 23 of the Departments 69 major information systems resulting in the issuance of two recommendations. Given how long ago the audit review was conducted, at the issuance of this report, most of the findings cited are not consistent with DOL’s current security posture, which has been consistently improving since 2015. While several of the individual instances cited in the report are accurate, management reasserts our previous view that OIG audit reporting conflates disparate and sometimes anomalous issues. This results in reporting that lacks the linkage between the findings and the risks that could be expected to rise the level of seriousness commanding immediate management attention. Further, in management’s view, the repeated reference to “lack of oversight” as the root cause of identified issues is not supported by documented evidence. Nevertheless, securing our information systems one of the Department’s highest priorities and the DOL Enterprise Security Program has made several advances in each of the areas referenced in the report.

During the months since the OIG’s review concluded, DOL has achieved many relevant successes that directly address the concerns cited in the report and are consistent with the intent of the audit report’s recommendations. One such effort proactively undertaken was the OCIO-Led Enterprise Cybersecurity Corrective Action Plan (CAP). The CAP was a concerted and rigorous effort to validate foundational improvements in the areas of Access Management, Vulnerability Management, Configuration Management, and Third Party Oversight. In many instances, the CAP further required immediate security control implementation such as: modification to access control procedures including requiring out of cycle user account reviews (privileged and general user accounts) be performed resulting in immediate improvement. The CAP also included specialized training, the development of reporting and accountability measures as well as the issuance of formal policy and procedure updates to address the identified deficiencies.

DOL’s Enterprise Security Operations team has made great progress in architecting and introducing new security capabilities. Among the recent progress includes but is not limited to the following Cybersecurity program enhancements:

- Expansion of network security monitoring services to include web content filtering, Intrusion Detection and Prevention, Internet Anti-virus blocking and network inspection.
- Deployment of several new security tools including WebInspect, DBProtect, Nessus Security Center, BigFix Software Utilization Analysis (SUA), and Fortify.
- Implementation of weekly Enterprise Cybersecurity Patch and vulnerability dashboard reports
- Completion of bi-annual Cybersecurity phishing and data exfiltration exercises.

Also, the statement: “However, the PIV cards were not implemented until July 15, 2015 in response to an OMB mandate” does not acknowledge the full context of the Department’s IAM program PIV card implementation efforts as communicated to the OIG. The Department’s Identity and access management program was chartered and approved by the DOL IT Project Review Board in Q2 FY 2014. Through collaborative efforts, the IAM led the DOL IAM technical working group in implementing the foundational network components such as updates to DOL’s Active Directory, the implementation of DOL’s Public Key Infrastructure and the deployment of PIV card logon to all DOL users. Continuing efforts as outlined in DOL’s implementation strategy, DOL was able to implement the next phase of its IAM program by enforcing the use of the PIV card for 91% of its general users, surpassing the Federal Cybersprint target and 94% of its privileged users. It is important to recognize that DOL reallocated a tremendous amount of resources to accelerate its implementation strategy in the achievement of the Cybersprint targets, despite not receiving the requested IAM program budget.

Cybersecurity is one of the Department’s highest priorities and management is committed to ensuring the security of our information and information systems and management will continue efforts to ensure corrective action plans – to which the OIG has full access -- are developed and implemented to address the identified deficiencies. DOL will also continue its planned implementation of proactive enterprise security solutions enabling enhancements to its Information Security Continuous Monitoring program.

Management acknowledges the OIG’s recommendation to realign the organization structure as it relates to the CIO to address the organization independence issue identified in the report. Management asserts the CIO reporting structure is defined in a way that best works for the Department and is aligned with the Office of Management and Budget’s Federal Information Technology Acquisition Reform Act CIO assignment plan.

We appreciate the opportunity to provide input and look forward to 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](mailto:manning.tonya@dol.gov) or (202) 693-4431.

cc: T. Michael Kerr, ASAM  
Ed Hugler, ASAM  
Gundeep Ahluwalia, D/CIO  
Tonya Manning, OCIO  
Keith Galayda, OIG

**APPENDIX C**

---

**ACRONYMS**

---

CIGIE	Council of the Inspectors General on Integrity and Efficiency
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 Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
FY	Fiscal Year
GAO	Government Accountability Office
ISSO	Information Systems Security Officer
IT	Information Technology
OASAM	Office of the Assistant Secretary for Administration and Management
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action & Milestones
Q	Quarter
RTO	Recovery Time Objective
SCA	Security Controls Assessment
SOD	Separation of Duties
SP	Special Publication
US-CERT	United State Computer Emergency Readiness Team

**APPENDIX D**

---

**ACKNOWLEDGEMENTS**

---

Key contributors to this report were: Keith Galayda (Audit Director), Ethan Iczkovitz (Audit Manager), Christian Arsenault, and LeslieAntoinett Hunter.



**TO REPORT FRAUD, WASTE OR ABUSE, PLEASE CONTACT:**

Online: <http://www.oig.dol.gov/hotlineform.htm>

Email: [hotline@oig.dol.gov](mailto: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