U.S. Department of Labor

Office of Inspector General—Office of Audit

REPORT TO THE CHIEF INFORMATION OFFICER

REPORT ON U.S. DEPARTMENT OF LABOR'S POLICIES AND GUIDELINES IN ACCORDANCE WITH THE CYBERSECURITY ACT OF 2015, SECTION 406

Date Issued: August 15, 2016
Report Number: 23-16-007-07-720

TABLE OF CONTENTS

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210

August 15, 2016

INSPECTOR GENERAL'S REPORT

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

This report presents the results of our work conducted to identify what U.S. Department of Labor (DOL) policies and guidelines were in place for the 62 systems DOL reported as subject to Section 406 of the Cybersecurity Act (CSA) of 2015, as of August 10, 2016. The CSA was enacted on December 18, 2015, and is intended to help prevent cybercrimes, such as information and identity theft.

Our work was completed in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation. We performed this work during the period March 1, 2016, to August 11, 2016, and reviewed policies and guidelines that were in effect during this period.

On December 18, 2015, the President signed the CSA. Section 406 of the CSA focuses on cybersecurity logical access controls and information security management monitoring controls. Congress required the Inspectors General under the Fiscal Year (FY) 2016 Appropriation Act of January 6, 2016, to submit a report on the security controls identified in Section 406 for information systems that provide access to personally identifiable information (PII) no later than 240 days after enactment.

The objective of our work was to determine if DOL had policies and guidelines in place that complied with Section 406. We did not perform any work to determine the operating effectiveness of the controls and, therefore, express no opinion on such.

Our methodology in performing the work included collecting information regarding the design of the DOL IT cybersecurity-related policies and guidelines for the 62 systems DOL identified as containing PII and therefore subject to the requirements of Section 406. We inquired of management and inspected the policies and guidelines established at DOL. We leveraged information from the FY 2016 Federal Information Security Modernization Act evaluation and other OIG reports for Section 406 cybersecurity areas. See Appendix A for details regarding our objective, scope, methodology, and criteria.

We reviewed the contents of this report with the Office of the Chief Information Officer and this report reflects our consideration of their feedback. The results of our work will be incorporated in the Inspector General's FY 2016 Federal Information Security Modernization Act (FISMA) report issued to the Secretary of Labor, which will include any observations, concerns and recommendations related to DOL's cybersecurity controls.

RESULTS IN BRIEF

As of August 10, 2016, DOL reported that it had 62 systems containing PII and therefore subject to the requirements of Section 406 (see Exhibit for a listing of these systems). DOL had policies and guidelines in place that complied with the requirements of Section 406, except for gaps in the following areas:

- Two information systems did not follow personal identity verification (PIV) multi-factor authentication for privileged users per the DOL Computer Security Handbook (CSH).

- DOL lacked automated tools for monitoring information systems for unauthorized access and had no automated capabilities for data loss prevention, visibility (i.e., allows for detection of which applications are accessed within the organization irrespective of their ports and protocols), or digital rights management.

DOL is at increased risk of malicious attacks in systems that do not use multi-factor authentication. Additionally, no automated capabilities and tools to perform continuous monitoring raises the risk of unauthorized access to networks and systems.

Additional details of our observations and concerns, and the specific systems to which they relate, were provided to the CIO under separate cover.

The results of this Section 406 cybersecurity assessment will be incorporated into the FY 2016 FISMA evaluation and any specific recommendations to remediate and mitigate weaknesses identified.

BACKGROUND

On December 18, 2015, the President signed the CSA into law. Over the past several years, major cyberattacks, such as the attack on the Office of Personnel Management that exposed the personal information of over 20 million current, former and prospective

federal employees, have raised public awareness of the importance of online security. The CSA is intended to help prevent further cyberattacks.

Section 406 of the act focuses on federal agencies' cybersecurity logical access controls and information security management monitoring controls. Congress required Inspectors General to submit a report on selected security controls identified in Section 406 for covered systems. Covered systems comprise national security systems as defined in Section 11103 of title 40, United States Code and federal computer systems that provide access to PII. Specifically, Section 406 states for each Inspector General to report the following:

- Description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.
- A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.
- If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.
- A description of specified information security management practices used by the covered agency regarding covered systems.
- A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices.

RESULTS

As of August 10, 2016, DOL reported that it had 62 systems containing PII and therefore subject to the requirements of Section 406 (see Exhibit for a list of these systems). DOL had policies and guidelines in place for the 62 covered systems that complied with the requirements of Section 406, with two exceptions: (1) two information systems did not follow PIV multi-factor authentication for privileged user access per the DOL CSH; and (2) DOL had no automated tools for monitoring information systems for unauthorized access and did not have automated capabilities for data loss prevention, visibility (i.e., the ability to detect which applications are accessed and by whom) or digital rights management.

In the two systems that were not using multi-factor authentication, DOL was at increased risk of malicious attacks. The lack of automated capabilities and tools to perform continuous monitoring hampered DOL's ability to protect its networks and systems from unauthorized access.

DOL Compliance with Section 406 Requirements

We determined if DOL had policies and guidelines in place that complied with the following five areas defined in Section 406:

1. **Description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.**

   The DOL Computer Security Handbook (CSH), Edition 5.0, Volume 7, *Identification and Authentication Policies, Procedures, and Standards*, dated February 19, 2015, specified the department standards governing logical access. While every DOL agency was required to comply with the minimum logical access policies and standards specified by the CSH, a number of agencies have adopted additional logical access policies and guidelines to enhance the standards specified by the CSH.

   Identified Gap: Based on survey results for the 62 covered information systems reported by DOL, we identified two information systems that did not follow PIV multi-factor authentication for privileged users (i.e., a user who has access to system control, monitoring, or administrative functions) per the CSH.

2. **A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.**

   DOL's CSH, Edition 5.0, Volume 7, *Identification and Authentication Policies, Procedures, and Standards*, dated February 19, 2015, specifies DOL's required minimum standards on managing information system identification and authentication of DOL users as follows:

   a) Authentication of users must be accomplished through the use of passwords, tokens, biometrics, or in the case of multi-factor authentication, some combination therein;
   b) Multi-factor authentication must be used for network access to privileged accounts; and
   c) The information system must use multi-factor authentication for local access to privileged accounts.

DOL's additional minimum required standards on managing information system user identification and authentication of DOL users for Moderate and High information systems are as follows:

a) The information system implements multi-factor authentication for network access to privileged and non-privileged accounts;
b) The information system implements multi-factor authentication for local access to privileged and non-privileged accounts;
c) The information system implements replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts;
d) The information system implements multi-factor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device minimally meets Assurance Level 3 as defined in OMB Memorandum 04-04; and
e) The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

3. If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

Based on survey results for the 62 covered information systems identified by DOL, 8 systems reported they do not have privileged application users. Of the 54 systems that identified as having privileged users, 52 systems either maintain the same process for both privileged and general users to be granted access via multi-factor authentication or inherit multi-factor authentication controls through the supporting general support system.

Identified Gap: Two of the 62 covered information systems identified by DOL had not implemented multi-factor authentication methods. DOL officials stated these systems were not able to implement PIV access with their current technological capabilities. One of the two systems had a plan of action and milestone in place to remediate the deficiency and the other system could not be configured for PIV access.

4. A description of the following information security management practices used by the covered agency regarding covered systems:

a. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

Regarding the software inventory process, DOL's CSH, Edition 5.0, Volume 20,

Inventory Methodology Policies and Standards: The DOL Inventory of Major Information Systems, dated February 19, 2015, states:

> The annual inventory process entails the use of the Cyber Security Assessment and Management (CSAM) tool. The DOL process for categorizing DOL information and information systems will leverage CSAM's capabilities of categorizing the information types according to the latest version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1.* As part of this process, agency officials shall use the security categorizations standards for systems listed in Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*.
>
> To complete the annual inventory assessment in CSAM, DOL agencies must ensure that the system categorization questions and FIPS 199 information in the seven (7) CSAM screens (listed below) are accurate and updated, if necessary:
>
> 1. System Identification
> 2. Info Types (FIPS 199 using 800-60 Rev. 1)
> 3. Locations
> 4. Relationships
> 5. Narratives
> 6. POCs
> 7. Status & Archive

Regarding the software inventory and license process, the DOL CSH, Edition 5.0, Volume 5, *Configuration Management Policies, Procedures and Standards,* dated February 19, 2015, states:

> DOL's required minimum standards on developing and documenting an information system component inventory are as follows:
>
> 1. Agency information system personnel, authorized by the system owner, shall develop and document an inventory of information system components that:
>   a. accurately reflects the current information system
>   b. includes all components within the authorization boundary of the information system.
>   c. determine the appropriate level of granularity deemed necessary for tracking and reporting.

d. Includes system-specific information deemed necessary for effective accountability of information system components including, but is not limited to:
   i. Manufacturer
   ii. Model number
   iii. Serial number
   iv. Software license information
   v. System/component owner

2. DOL agencies must review and update the information system component inventory at least on an annual basis or when a system change occurs.

DOL's required minimum standards on implementing and enforcing software usage restrictions required DOL agencies to:

1. Use software and associated documentation in accordance with contract agreements and copyright laws.
2. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.
3. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

We were informed by DOL's OCIO that CSAM was the primary repository for information system inventories within DOL. For DOL's information systems, software was defined in the System Security Plan (SSP). The SSP was updated every three years or when a significant change was made to the configuration of the system. Annual reviews are conducted and records of the reviews were included in the SSP which were updated in CSAM. The current software inventory process was decentralized with system owners maintaining records of their own system software, including licensing, with guidance and oversight from DOL's OCIO.

b. What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including: data loss prevention capabilities; forensics and visibility capabilities; or digital rights management capabilities and a description of how the covered agencies are using those capabilities.

Regarding monitoring and detecting exfiltration and other threats, DOL's CSH, Edition 5.0, Volume 17, *System and Information Integrity Policies,* dated February 19, 2015, states:

> Information systems must implement intrusion detection tools and techniques which are capable of monitoring events on the information

system, detect attacks, and provide identification of unauthorized use of the system. The tools utilized in order to conduct intrusion detection include, but are not limited to, intrusion detection systems, virus protection software, log monitoring software, and network forensics analysis tools. Additionally, as a first line of defense, network protection may also be provided in the form of switches, routers, firewalls, etc.

At a minimum, DOL's standards on monitoring information systems require DOL to:

1. Monitor the information system to detect:
   a. attacks and indicators of potential attacks in accordance with DOL's Continuous Monitoring and Incident Response requirements identified herein and in additional DOL published guidance and standards; and
   b. Unauthorized local, network, and remote connections.
2. Identify unauthorized use of the information system through monitoring capabilities such as, but not limited to, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.
   (NOTE: Standards for enterprise tools may be defined by the DOL Continuous Monitoring Program)
3. Deploy monitoring devices both strategically within the information system to collect essential information and at ad hoc locations within the system to track specific types of transactions of interest to the Department.
4. Protect information obtained from monitoring tools from unauthorized access, modification, and deletion.
5. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to Department operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
6. Obtain a legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

DOL's minimum standards on monitoring Moderate and High information systems require DOL systems to:

7. Employ automated tools to support near real-time analysis of events.
8. Monitor inbound and outbound communications traffic in near real time for unusual or unauthorized activities or conditions.

9. Alert agency and/or enterprise designated individuals when agency-defined indications of compromise or potential compromise occur (such as irregular resource consumption or audit function disablement).

Regarding monitoring and detecting exfiltration and other threats, DOL's CSH, Edition 5.0, Volume 17, *System and Information Integrity Policies,* dated February 19, 2015 states:

> The information system must detect unauthorized changes to software, firmware, and information. DOL's required minimum standards on software, firmware, and information integrity for Moderate information systems are as follows:
>
> 1. The information system reassesses the integrity of software, firmware, and information by performing at least monthly integrity scans of the information system.
> 2. The information system must employ integrity verification applications to look for evidence of information tampering, errors, and omissions.
> 3. Good software engineering practices must be employed on the information system with regard to commercial off-the-shelf integrity mechanisms (including but not limited to parity checks, cyclical redundancy checks, and cryptographic hashes) and must use tools to automatically monitor the integrity of the information system and the applications it hosts.
> 4. The information system must implement a capability to detect to the extent possible and prevent any accidental or intentional changes to software (including but not limited to operating systems, middleware, software), firmware (including but not limited to Basic Input Output Systems (BIOS)), and information (such as metadata) used to complete the system's business functions.
> 5. The organization incorporates the detection of unauthorized software, firmware, and information changes into the incident response capability. The detection capability must ensure unauthorized changes are tracked, monitored, corrected, and available for historical purposes.

DOL's minimum standards on software, firmware, and information integrity for High information systems require DOL systems to:

1. Employ automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

2. Employ automated tools that provide notification to organizational personnel (such as but not limited to business owners, information system owners, system administrators, software developers) upon discovering discrepancies during integrity verification.
3. Automatically shut down and restarts the information system, and implements security safeguards when integrity violations are discovered.

And require DOL to:

4a. Prohibit the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and
4b. Provide exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

Regarding monitoring and detecting exfiltration and other threats, DOL's CSH, Edition 5.0, Volume 8, *Incident Response Policies, Procedures, and Standards,* dated February 19, 2015, states:

> Agencies must provide and incident response support resource, integral to the organizational incident response capability.

DOL's required minimum standard on managing incident response was as follows:

> The incident response support resource offers assistance and advice to users of the information system for the handling and reporting of security incidents. Incident response support resources provided by agencies include, for example, help desks, assistance groups, and access to forensics services, when required. The incident support resource should support the agency's overall incident response capabilities.

DOL's additional required minimum standard on incident response support for Moderate and High information systems was as follows:

> Automated mechanisms (including but not limited to automated answering and/or ticketing system for help desk, RSS and Atom feeds, subscriptions, distribution lists, etc.) must be employed to increase availability of incident response-related information and support.

Regarding monitoring and detecting exfiltration and other threats, DOL's CSH, Edition 5.0, Volume 8, *Incident Response Policies, Procedures, and Standards,* dated February 19, 2015, states:

Security incidents must be documented and tracked.

DOL's required minimum standards on incident monitoring were as follows:

1. All security incidents must be reported to DOLCSIRC. DOLCSIRC will maintain a log of all incidents that occur at DOL.
2. Agency response teams are required to maintain their own logs of incident reports submitted to DOLCSIRC for a period of no less than three years.
3. Security incidents must be documented and tracked to include information such as the status of the incident and other pertinent information necessary for forensics, evaluating incident details, trends, and handling.

DOL's additional required minimum standards on managing information system Incident Monitoring for High information systems were as follows:

1. Automated mechanisms must be used to assist in the tracking of security incidents. These automated mechanisms must also assist in the collection and analysis of information regarding security incidents.
2. Automated mechanisms for tracking security incidents and collecting / analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents.

c. If the covered agency is not utilizing capabilities described above, a description of the reasons for not utilizing such capabilities.

DOL relied primarily on a Managed Trusted Internet Protocol Service (MTIPS) to alert DOL of any possible data exfiltration.

Identified Gap: The OCIO indicated a lack of resources for automated tools made it difficult to monitor information systems within the Department.

5. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices.

Regarding Contractor Monitoring, DOL's CSH, Edition 5.0, *Introduction*, dated February 19, 2015, states:

> This handbook is primarily a DOL document. The policies, procedures, and standards, and format are not binding on external organizations that have interconnectivity with DOL systems. A Memorandum of Understanding (MOU) and / or Interconnection Security Agreement (ISA) should be in place for these connections.
>
> The policies, procedures, and standards are binding on all operators of DOL systems. An "operator" of a DOL system is any individual or organization who processes, stores, or transmits information on a DOL system on behalf of DOL to accomplish a DOL function. An example of a DOL operator who is not a DOL employee is a local or state government employee or contractor processing information on behalf of DOL to accomplish a DOL business or IT function.

DOL's CSH, Edition 5.0, Volume 0, *Information Security Policies,* dated February 19, 2015, states:

> DOL information users (Executive, Federal Employees and Contractor Staff) are expected to review and comply with all DOL policies, procedures, and standards contained in the DOL Manual Series (DLMS) and the CSH, to include, but not be limited to, training for information systems security, privacy awareness, and role-based training for individuals who hold positions with significant privacy roles and responsibilities.

Regarding the usage of external systems, DOL's CSH, Edition 5.0, Volume 1, *Access Control Policy, Procedures, and Standards,* dated February 19, 2015, states:

> DOL agencies establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
>
> a. Access the information system from the external information systems
> b. Process, store, and/or transmit agency-controlled information using the external information systems

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the agency and for which the agency typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (including but not limited to, computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (including but not limited to, hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and Federal information systems that are not owned by, operated by, or under the direct supervision and authority of the agency.

For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to those agencies, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies.

Authorized individuals include agency personnel, contractors, or any other individuals with authorized access to the agency information system and over which the agency has the authority to impose rules of behavior with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local, or tribal government.

This policy does not apply to the use of external information systems to access public interfaces to agency information systems and information that are intended for public access (including but not limited to, individuals accessing Federal information through public interfaces to agency information systems). Refer to NIST SP 800-46 and 800-77 for guidance on the use of external information systems.

OCIO stated at the enterprise level, DOL provides quarterly newsletters and specialized quarterly role-based training in DOL's policies, procedures and standards that are leveraged by information system owners resulting in cost benefits to the agencies. DOL policy requires all contractors abide by the CSH and DOL's Rules of Behavior. OCIO informed OIG that legal contract language may impede the swift implementation of changing security requirements for contracted services. Additionally, the OCIO published a Third Party Security Monitoring Guide to provide additional guidance to the functions associated with contractor monitoring.

Identified Gap: DOL has encryption controls in place for protecting data and preventing data loss, but there are no automated capabilities for data loss prevention, visibility, or digital rights management.

We appreciate the cooperation and assistance the Chief Information Officer, DOL agencies and staffs provided to the OIG in performing the above work.

Elliot P. Lewis
Assistant Inspector General
for Audit

Exhibit

EXHIBIT

LIST OF 62 COVERED SYSTEMS REPORTED BY DOL
(as of August 10, 2016)

#	Bureau of Labor Statistics
1	Consumer Price Index
2	LABSTAT
3	LAN/WAN Infrastructure
4	Management Information System
5	National Longitudinal Survey
6	Occupational Safety and Health Statistics System
#	**Department of the Secretary**
7	DOL Appeals Management System
#	**Employee Benefits Security Administration**
8	Employee Retirement Income Security Act Filing Acceptance System
9	Enforcement Management System
10	Technical Assistance and Inquiries System
#	**Employee & Training Administration**
11	Cloud Platform Services
12	Enterprise Business Support System
13	ETA Business Process Management Platform
14	Foreign Labor Certification System
#	**Job Corps**
15	Student Pay Allotment Management Information System
#	**Mine Safety & Health Administration**
16	MSHA Standardized Information System
#	**Office of Administrative Law Judges**
17	Case Tracking System
#	**Office of the Assistant Secretary for Administration & Management**
18	AlertFind by MessageOne
19	Cloud CRM Solution
20	Departmental E-Business Suite
21	DOL Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification II System
22	Employee Computer Network/Departmental Computer Network
23	Labor Employee Relations Management Systems 2.0
24	Master Data Repository
25	Safety & Health Information Management System - Hosting Version 4
26	Secretary's Information Management System
27	Title-VI / VII Processing System
#	**Office of the Chief Financial Officer**
28	New Core Financial Management System

#	Office of Disability Employment Policy
29	Workforce Recruitment Program
#	**Office of Federal Contract Compliance Programs**
30	OFCCP Information System
#	**Office of Inspector General**
31	Electronic Office of the Inspector General System
32	Teammate
#	**Office of Labor-Management Standards**
33	Electronic Labor Organization Reporting System
#	**Office of Public Affairs**
34	DOL Contact Us
35	DOL EmailFriend
36	DOL Events Calendar
37	DOL National Contact Center
38	Employment Laws Assistance for Workers and Small Businesses
39	LaborNet Events Calendar
40	News Releases Log
41	Ride Sharing System
42	Small Business Vendor Outreach Session (Registration)
43	Web Production Environment System
44	Wiki
#	**Occupational Safety & Health Administration**
45	Integrated Management Information System – Legacy
46	OSHA Business Information System
47	OSHA Information System
48	OSHA Web Services
49	Web Integrated Management Information System
#	**Office of Workers' Compensation Programs**
50	Automated Support Package
51	Central Bill Processing
52	Integrated Federal Employees' Compensation System
53	Longshore Case Management System
54	Longshore Disbursement System
55	OWCP Workers' Compensation System
#	**Office of the Solicitor**
56	Evidence Management System
57	Matter Management System
#	**Veterans Employment & Training Service**
58	Veterans' Data Exchange Initiative
59	Veterans Investigative Preference and Employment Rights System
#	**Wage and Hour Division**
60	Back Wage Financial System
61	Civil Money Penalty
62	Wage and Hour Investigative Support System and Reporting Database

Appendices

APPENDIX A

OBJECTIVE, SCOPE, METHODOLOGY, AND CRITERIA

OBJECTIVE

The objective of our work was to determine whether DOL had policies and procedures in place that complied with Section 406. We did not perform any work to determine the operating effectiveness of the controls and, therefore, express no opinion on such.

SCOPE

OIG conducted this work in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation. As of August 10, 2016, DOL identified 62 systems (see Exhibit) as containing PII and therefore subject to the requirements of Section 406. We reviewed these 62 systems during the period March 1, 2016, to August 11, 2016, and reviewed policies and procedures that were in effect during this period. The work was performed at DOL facilities located in Washington, DC.

METHODOLOGY

As part of this assessment, we obtained and inspected the System Security Plans (SSPs) for the 62 systems DOL reported as covered by Section 406, and sent a survey questionnaire to the system owners inquiring of the policies and procedures followed for granting and approving logical access requests and for requiring privileged users to authenticate to the system using a PIV card. We also inquired of the OCIO to understand some of the various policies and procedures in place related to DOL-wide security management and contractor monitoring. We did not test the operating effectiveness of controls as part of this assessment.

As part of the CSA Section 406 assessment, we reviewed all 62 DOL information systems that DOL identified as covered systems[1] as defined by Section 406. We identified a listing of 62 DOL information systems that contain PII. We used these systems to focus the Section 406 report and to provide an understanding of DOL's cybersecurity policies and guidelines. For the listing of systems evaluated for this report, see the Exhibit.[2]

[1] A "covered system" is defined as a national security system as defined in Section 11103 of Title 40, United States Code or Federal computer systems that provide access to PII.
[2] The list of 62 DOL information systems was generated from DOL's central repository Cyber Security Assessment & Management (CSAM) tool on August 10, 2016.

CRITERIA

This work was performed to comply with the requirements of Section 406 of the Cybersecurity Act of 2015, as follows:

SEC. 406. FEDERAL COMPUTER SECURITY.

a) DEFINITIONS.—In this section:

1) COVERED SYSTEM.—The term ‘‘covered system’’ shall mean a national security system as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.
2) COVERED AGENCY.—The term ‘‘covered agency’’ means an agency that operates a covered system.
3) LOGICAL ACCESS CONTROL.—The term ‘‘logical access control’’ means a process of granting or denying specific requests to obtain and use information and related information processing services.
4) MULTI-FACTOR AUTHENTICATION.—The term ‘‘multi-factor authentication’’ means the use of not fewer than 2 authentication factors, such as the following:
   a. Something that is known to the user, such as a password or personal identification number.
   b. An access device that is provided to the user, such as a cryptographic identification device or token.
   c. A unique biometric characteristic of the user.
5) PRIVILEGED USER.—The term ‘‘privileged user’’ means a user who has access to system control, monitoring, or administrative functions.

b) INSPECTOR GENERAL REPORTS ON COVERED SYSTEMS.—

1) IN GENERAL.—Not later than 240 days after the date of enactment of this Act, the Inspector General of each covered agency shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report, which shall include information collected from the covered agency for the contents described in paragraph (2) regarding the Federal computer systems of the covered agency.
2) CONTENTS.—The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:
   A. A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed

B. A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

C. If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

D. A description of the following information security management practices used by the covered agency regarding covered systems:

4. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

5. What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

I. data loss prevention capabilities;

II. forensics and visibility capabilities; or

III. digital rights management capabilities.

6. A description of how the covered agency is using the capabilities described in clause (ii).

7. If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

E. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

3) EXISTING REVIEW.—The reports required under this subsection may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the covered agency, and may be submitted as part of another report, including the report required under section 3555 of title 44, United States Code.

4) CLASSIFIED INFORMATION.—Reports submitted under this subsection shall be in unclassified form, but may include a classified annex.

APPENDIX B

LIST OF ACRONYMS

Acronym	Definition
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CSA	Computer Security Act
CSAM	Cyber Security Assessment and Management
CSH	Computer Security Handbook
DOL	Department of Labor
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification

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