DOL-OIG Highlights

November–December 2019

Highlighted Concern

The Office of Inspector General (OIG) identifies on an ongoing basis areas of significant concern that cause the U.S. Department of Labor (DOL) to be at particular risk of fraud, mismanagement, waste, deficiencies, or abuse. Below is one of our current concerns. Please visit our Significant Concerns page to learn about all DOL-OIG significant concerns.

Securing and Protecting Information Management Systems

For many years, we have reported on long-standing information security deficiencies, including weaknesses in third-party oversight, incident response and reporting, risk management, and continuous monitoring. For example, DOL needs to improve in the following areas:

- provide adequate oversight of its systems that are either owned or operated by contractors or other federal entities on behalf of DOL;
- promptly report its computer security incidents to the DOL Computer Security Incident Response Capability and the United States Computer Emergency Readiness Team for investigation and action;
- accurately determine its system inventory, as well as its hardware and software asset inventory; and
- implement a program to identify system security vulnerabilities and ensure that appropriate actions are being taken.

Open Recommendations

as of February 3, 2020

222	**$180,734,486**
Open Recommendations	Monetary Value of Recommendations

Recommendation Dashboard

These deficiencies represent ongoing, unnecessary risks to the confidentiality, integrity, and availability of DOL's information within the information systems that support DOL's mission.

We have recommended that the Department place greater emphasis on these deficiencies and prioritize available resources to address them. We likewise recommended realigning the position of the Chief Information Officer (CIO) to report directly to the agency head. Such a realignment will provide the CIO with greater independence and authority to implement and maintain an effective information security program.

Reports Issued

Special Report Relating to the Federal Employees' Compensation Act Special Benefit Fund
Report No. 22-20-003-04-431
(November 1, 2019)

A special report relating to the Federal Employees' Compensation Act (FECA) Special Benefit Fund disclosed a deficiency in internal controls over reporting of a benefit expense, but the deficiency was not considered a material weakness. Testing of compliance disclosed no instances of noncompliance.

District of Columbia Workmen's Compensation Act Special Fund
Report No. 22-20-002-04-432
(November 14, 2019)

We performed an audit on the financial statements of the District of Columbia Workmen's Compensation Act Special Fund, and found that the financial statements were presented fairly in accordance with U.S. generally accepted accounting principles.

Longshore and Harbor Workers' Compensation Act Special Fund
Report No. 22-20-001-04-432
(November 14, 2019)

We performed an audit on the financial statements of DOL's Longshore and Harbor Workers' Compensation Act Special Fund, and found that the financial statements were presented fairly in accordance with U.S. generally accepted accounting principles.

Stronger Controls Needed over Web Application Security
Report No. 23-20-001-07-725
(November 14, 2019)

We found that DOL did not implement sufficient control activities to monitor and secure its publicly accessible Web applications.

Independent Auditors' Report on the DOL Financial Statements
Report No. 22-20-004-13-001
(November 18, 2019)

An independent auditors' report on DOL's consolidated and sustainability financial statements found that the financial statements were presented fairly in accordance with U.S. generally accepted accounting principles.

DOL's Reported Data Generally Met Quality Standards, but Accuracy Issues Remain
Report No. 03-20-001-13-001
(November 21, 2019)

We performed an audit of DOL's reported data under the Digital Accountability and Transparency Act of 2014, and found 94 percent accuracy of DOL's reported data, which according to the government-wide methodology indicated that the data were of high quality.

FY 2019 FISMA DOL Information Security Report: Implementation of Security Tools Hindered by Insufficient Planning
Report No. 23-20-002-07-725
(December 23, 2019)

An independent evaluation of the DOL fiscal year (FY) 2019 information security programs determined, according to the Department of Homeland Security's FISMA reporting system calculation, DOL's information security program was not effective for FY 2019.

Investigations

A Rochester, NY man pleaded guilty to defrauding investors around the country as part of a Ponzi scheme that resulted in a total loss to investors of $70.7 million.
(USAO MD-PA 11/05/19)

A senator representing Puerto Rico was indicted for bribery concerning programs receiving federal funds.
(USAO D-PR 11/06/2019)

A former Atlanta Regional Commission employee was arraigned on charges of bribery and extortion.
(USAO ND-GA 11/08/2019)

A Cleveland, North Dakota, woman pleaded guilty to false statement, false swearing in an immigration matter, and mail fraud.
(USAO D-ND 11/14/2019)

A California man was sentenced to four years in prison for criminal conspiracies to submit false claims for federal income tax refunds and to commit mail fraud in connection with California state unemployment insurance benefits.
(USAO ED-CA 11/19/2019)

Two former Baltimore City employees pleaded guilty to conspiracy to commit wire fraud, conspiracy to defraud the United States, and filing a false tax return.
(USAO D-MD 11/20/2019)

A doctor who practiced in New Jersey and Pennsylvania pleaded guilty to participating in a scheme to receive over $140,000 in bribes and kickbacks from a pharmaceutical company.
(USAO D-NJ 11/20/2019)

A Chicago and Arlington, Tennessee, man was convicted of two counts of conspiracy, 12 counts of mail fraud, 10 counts of money laundering, and four counts of identity theft related to a veteran's unemployment compensation fraud scheme.
(USAO MD-PA 11/25/2019)

A San Antonio businessman was sentenced to seven years in federal prison for his role in a multi-million-dollar health care fraud scheme.
(USAO WD-TX 12/02/2019)

A member of the Genovese Crime Family was convicted of conspiring to commit extortion and racketeering offenses with other members and associates of the family.
(USAO SD-NY 12/4/2019)

A former high-level United Automobile Workers (UAW) official pleaded guilty to conspiring with other UAW officials to engage in honest services fraud by taking $250,000 in bribes and kickbacks from a UAW vendor and and to conspiring to launder the proceeds of the scheme.
(USAO ED-MI 12/04/2019)

A former California Employment Development Department employee pleaded guilty for her role in a scheme to defraud the State of California by filing false unemployment insurance claims. (USAO ED-CA 12/10/2019)

A Texas woman was convicted for her role in a $5.5 million scheme to overbill the DOL Office of Workers' Compensation Programs for physical therapy and other services. (DOJ News Release 12/13/2019)

A Portland, Maine, woman was sentenced to 12 months and one day in prison for embezzling from an employee benefit plan. (USAO D-ME 12/18/19)

A New York man was arraigned on 10 counts of wire fraud and one count of embezzling funds from an employee benefit plan. (USAO ND-NY 12/19/19)