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

# BRIEFLY…

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

## WHY READ THE REPORT

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

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

## WHY OIG CONDUCTED THE AUDIT

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

## READ THE FULL REPORT

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

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

**March 2015**

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

## WHAT OIG FOUND

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

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

## WHAT OIG RECOMMENDED

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

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