# HIGHLIGHTS

## *Fiscal Year 2014 Evaluation of DHS' Compliance with Federal Information Security Management Act Requirements for Intelligence Systems*

# Unclassified Summary

**February 13, 2015**

We evaluated the Department of Homeland Security's (DHS) enterprise-wide security program for Top Secret/Sensitive Compartmented Information intelligence systems. Pursuant to the *Federal Information Security Management Act*, we reviewed the Department's security program including its policies, procedures, and system security controls for enterprise-wide intelligence systems. In doing so, we assessed the Department's continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, plans of actions and milestones for correcting information security weaknesses, contingency planning, and security capital planning.

Since our fiscal year 2013 evaluation, the Office of Intelligence and Analysis (I&A) has continued to provide effective oversight of DHS' department-wide intelligence systems and established programs to monitor ongoing security practices. For example, I&A has updated its policies and procedures, including publication of *DHS Sensitive Compartmented Information Systems Policy Directive 4300C* in September 2013. The United States Coast Guard (USCG) has relocated its headquarters to the St. Elizabeth's Campus and migrated to a new intelligence system that is now supported by the Defense Intelligence Agency, DHS, and USCG.

We identified deficiencies in I&A's configuration management and USCG's continuous monitoring, configuration management, risk management, security training, and contingency planning. We conducted our fieldwork from May through August 2014.



**For Further Information:**
Contact our Office of Public Affairs at (202) 254-4100 or email us at DHS-OIG.OfficeofPublicAffairs@oig.dhs.gov.