Office of Inspector General

(U) Review of DHS' Information Security Program for Intelligence Systems for Fiscal Year 2012

Unclassified Summary

We reviewed the Department of Homeland Security's (DHS) enterprise-wide security program and practices for Top Secret/Sensitive Compartmented Information intelligence systems. Pursuant to the Federal Information Security Management Act, we reviewed the department's security management, implementation, and evaluation of its intelligence activities, 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, contingency planning, security capital planning, and systems inventory.

Since the fiscal year 2011 evaluation, the Office of Intelligence and Analysis (I&A) has improved its oversight of department-wide systems and established programs to monitor ongoing security practices. I&A has developed and implemented a training program to educate DHS' growing number of personnel assigned security duties on intelligence systems. In addition, progress has been made in collaboration with other DHS components in centralizing plans and priorities for mitigating security weaknesses, streamlining system configuration management, and maintaining a systems inventory. However, we identified deficiencies in the areas of system authorization, supply chain threats, and security capital planning. Fieldwork was conducted from April through July 2012.