Department of Homeland Security
Office of Inspector General

Management Oversight Challenges Remain for DHS' Intelligence Systems Information Technology Security Program

Unclassified Summary

OIG-09-30

February 2009

Office of Inspector General
Management Oversight Challenges Remain for DHS' Intelligence Systems Information Technology Security Program
OIG-09-30

We evaluated the security program and practices for the Department of Homeland Security's Top Secret/Sensitive Compartmented Information systems according to Federal Information Security Management Act (FISMA) annual requirements. We focused on the security program management, implementation, and system administration of the department's intelligence systems. We primarily assessed the department's Plan of Action and Milestones (POA&M), system certification and accreditation, and incident reporting processes, as well as its security awareness training program.

The objective of our evaluation was to determine whether the department is properly protecting Top Secret/Sensitive Compartmented Information and the systems that support the department's intelligence operations and assets. We assessed the effectiveness of the information systems security controls for the department's intelligence systems, and the remediation of the findings that we reported as a result of our Fiscal Year 2007 assessment. This is the department's first year reporting on U.S. Coast Guard's (USCG) FISMA compliance. Fieldwork was conducted from May through October 2008, at the Intelligence and Analysis (I&A) and USCG.

The department continues to improve and strengthen its security programs for its intelligence systems. During the past year, the department finalized its Sensitive Compartmented Information Systems Information Assurance Handbook, which provides department intelligence personnel with security procedures and requirements to administer its intelligence systems and the information processed. The handbook is accompanied by policies and procedures pertaining to POA&M, incident reporting, and systems security plan development processes. Additionally the department certified and accredited its classified network extension. Furthermore, USCG intelligence systems were re-aligned under the purview of I&A. Subsequently, I&A accepted the existing USCG's intelligence systems certifications granted by the Department of Navy.

As a direct result of I&A's efforts in addressing last year's systems security vulnerabilities and recommendations, DHS instituted a comprehensive vulnerability and patch management program. In implementing this program, DHS has significantly minimized the security risks associated with the department's intelligence systems. The department addressed ten of the fourteen recommendations cited in our FY 2007 report.

Overall, information security procedures have been documented and controls have been implemented, providing an effective level of security for the department's intelligence systems. Yet, the department has not fully addressed the issues and remaining recommendations reported in our FY 2007 evaluation that remain open related to the POA&M process, the development of a contingency/disaster recovery plan and testing of controls, and the implementation of a formal information system security education, training, and awareness program for intelligence operations and personnel. Further, I&A has taken on the responsibility for the reporting of the USCG's compliance with the FISMA for its intelligence systems and should continue to provide management oversight to ensure that the USCG is maintaining its information technology security program. We recommended that the Under Secretary for I&A address the open recommendations and the Office of the Chief Information Officer address the system control issues that we identified during our review.

In response to our draft report, I&A concurred with our recommendations. I&A provided proposed plans of actions to address each of our recommendations. Additional clarification was needed to address the completion dates or in refining corrective actions to fully satisfy the intent of the proposed recommendations. Through subsequent discussion, I&A fully agreed with our concerns and has changed their proposed corrective actions. (OIG-09-30, February 2009, IT)

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.