DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Implementation Challenges Remain In Securing DHS Components' Intelligence Systems

Unclassified Summary

OIG-07-15

December 2006

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Office of Inspector General
Implementation Challenges Remain In Securing DHS Components' Intelligence Systems
OIG-07-15

We reviewed Top Secret/Sensitive Compartmented Information (TS/SCI) systems under the Department of Homeland Security's (DHS) purview. We focused on DHS' information assurance posture, including the policies and procedures in place for the department's intelligence systems. We performed our work at the departmental and organizational component levels, focusing on the system security controls for a subset of intelligence systems, according to the requirements in Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*.

The objective of our evaluation was to determine whether DHS' information security program and practices are adequate and effective in protecting the information and the systems that support DHS' intelligence operations and assets from unauthorized access, use, disclosure, disruption, modification, or destruction. We also determined whether DHS' privacy program and related activities pertain to its intelligence systems, and identified whether components have developed or incorporated requirements to protect intelligence system vulnerabilities into their classification guides. Furthermore, we conducted detailed assessments of security controls and documentation for DHS' intelligence systems and assessed the mitigation of system security weaknesses previously identified as a result of system security vulnerability assessments conducted for a subset of intelligence systems in Fiscal Years 2004 and 2005. Fieldwork was conducted from May through August 2006.

DHS formally established the Office of Intelligence and Analysis to implement the department's Information Technology security program for its intelligence systems and assets. We also identified issues regarding the certification and accreditation of DHS' intelligence systems; Plan of Action and Milestones process; incident detection, handling procedures, reporting, and analysis process; and information security training and awareness program for all users of intelligence systems and specialized training for employees with significant security responsibilities for DHS' intelligence systems. We recommended that DHS formally grant the Office of Intelligence and Analysis' Chief Information Officer the comprehensive authority to support the management, operation, and DCID 6/3 accreditation of the department's intelligence systems, excluding United States Coast Guard intelligence data systems. DHS management agreed with our recommendation and has begun taking actions to address the issues raised during our review. (OIG-07-15, December 2006)

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, 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 the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or e-mail DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.