DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Evaluation of DHS' Security Program and Practices For Its Intelligence Systems

Unclassified Summary

Office of Information Technology

OIG-06-13

December 2005

Office of Inspector General

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

Office of Inspector General
Evaluation of DHS' Security Program and Practices For Its Intelligence Systems
OIG-06-13

We conducted an evaluation of DHS' information assurance posture, including its policies and procedures, for the intelligence systems under the department's purview. We performed our work from May through September 2005, at both the program and organizational component levels. Our evaluation focused on DHS' compliance with the Federal Information Security Management Act of 2002 for its intelligence systems in operation as of May 1, 2005, and containing Top Secret/Sensitive Compartmented Information (TS/SCI).

The overall objective of our evaluation was to identify whether DHS' information security program and practices for its intelligence systems are adequate and effective in protecting TS/SCI information from unauthorized access, use, disclosure, disruption, modification, or destruction. Our assessment included five intelligence community-wide weakness areas that were previously identified by the Intelligence Community Chief Information Officer (IC CIO), and three additional areas that the IC CIO asked Offices of Inspector General to assess as part of their Fiscal Year 2005 review. As part of our evaluation, we also determined whether system security controls were adequate and effective for a sample of eight intelligence systems based upon the requirements in Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*. Additionally, we conducted system security vulnerability assessments for a subset of six of the eight intelligence systems included in our review. Furthermore, we evaluated DHS' Plan of Action and Milestones (POA&M) process for its intelligence systems and followed up on previous recommendations discussed with DHS.

We recommended that DHS establish a single, comprehensive, and inclusive information security program for its intelligence systems in order to: (1) address the issues identified; (2) provide adequate security for the information and information systems that support intelligence operations and assets; and (3) ensure the confidentiality, integrity, and availability of vital intelligence information. Both DHS' Office of Security and Assistant Secretary for Information Analysis concurred with our recommendation and have begun taking actions to address the issues identified.

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 email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.