Office of Inspector General

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

Office of Inspector General
Evaluation of DHS' Security Program for Its Intelligence Systems
OIG-05-04

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President on December 17, 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide security program. The agency's security program should provide security for the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The OIG performed an independent evaluation of DHS' security program for its intelligence systems as required by FISMA. The overall objective of our evaluation was to identify whether DHS' information security program and practices for its intelligence systems were adequate and effective in protecting the information from unauthorized access, use, disclosure, disruption, modification, or destruction. We performed our work at the program and organizational component levels, focusing on DHS' compliance with FISMA for its intelligence systems containing Top Secret/Special Compartmented Information, and in operation as of May 1, 2004. We also performed vulnerability assessments and tests of security controls for a sample of five DHS intelligence systems. Furthermore, we evaluated DHS' Plan of Action and Milestones process for its intelligence systems and assessed DHS' security training program.

Our review was conducted between April 2004 and July 2004 and represents a baseline evaluation of DHS' intelligence program according to FISMA. We recommended that DHS take certain steps to: (1) provide adequate security for the information and information systems that support its intelligence operations and assets; and (2) ensure the confidentiality, integrity, and availability of vital intelligence information. DHS concurred with our recommendations. We are posting only this summary on the OIG website because the report contains classified information and should not, consequently, be widely disseminated. This report contains additional administrative issues and recommendations that were not made a part of OIG-04-34.