

DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

**Survey of DHS Intelligence Collection
and Dissemination**
(Unclassified Summary)





Homeland
Security

June 5, 2007

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report surveys DHS intelligence collection and dissemination activities and capabilities, primarily outside the Washington, DC metropolitan area. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The issues identified herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

OIG

*Department of Homeland Security
Office of Inspector General*

Introduction

We surveyed the operational components of the Department of Homeland Security (DHS) Intelligence Enterprise to determine their respective missions, roles, responsibilities, and information sharing capabilities. Our specific focus was on the program and organizational components that produce raw information, intelligence-related information, or finished intelligence products.

The objectives of our survey were to (1) identify the activities within DHS that generate or disseminate intelligence-related information and each activity's mission, function, and capabilities; (2) determine the sources of information collected or obtained by the DHS intelligence enterprise activities, and how the information is collected or obtained; (3) determine the customers of DHS intelligence enterprise activities, and how products are disseminated; (4) determine how priority intelligence requirements are generated, and how they are tasked to DHS and non-DHS intelligence enterprise activities; and (5) identify issues for management action stemming from our survey of the DHS field intelligence enterprise. We conducted our fieldwork from November 2005 through January 2007, under the authority of the Inspector General Act of 1978, as amended, and according to the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency.

Background

The *Homeland Security Act of 2002* created DHS and intended the intelligence component of the department to be the focal point for all terrorism-related intelligence to protect the Nation.¹ The legislation specifically assigned primary responsibility to DHS for receiving and analyzing all available intelligence that contributes to understanding the nature and scope of the terrorist threat to the American homeland and to detect and identify potential threats of terrorism within the United States. The *Homeland Security Act of 2002* also tasked DHS with developing policies and procedures to govern the sharing of law enforcement and intelligence information relating to homeland security within the federal government and state and local governments.

¹ 6 U.S.C. § 101, *et seq.*

Since the enactment of the *Homeland Security Act of 2002*, reports by such agencies as DHS' Office of Inspector, the Government Accountability Office and Congressional legislation have identified the need for DHS to assume a greater role in integrating, coordinating, and sharing homeland security related information. The 9/11 Commission determined that the largest obstacle to "connecting the dots" was resistance within the federal government to information sharing.² As a result, the *Intelligence Reform and Terrorism Prevention Act of 2004* mandated the creation of a new information-sharing environment. The new act sought to lessen the resistance to sharing terrorism and homeland security intelligence among federal government agencies, and with state, local, and private sector entities.³

In early 2005, the DHS Secretary commissioned the Second Stage Review to identify issues and opportunities for improvement within the department. This review recommended changes to bolster DHS' intelligence and information sharing environment. The Second Stage Review Information and Intelligence Sharing Team noted that the department's intelligence components were not integrated. It observed that these components contained multiple points of collection without coordination of intelligence and information sharing standards or processes. The Second Stage Review further stated that DHS' intelligence and operational components were not meeting the needs of its stakeholders, which include other DHS components, the Intelligence Community and state, local, and private sector entities.

In response to the Second Stage Review findings, the Secretary reorganized the department-level intelligence components by creating the DHS Office of Intelligence and Analysis, led by the Chief Intelligence Officer for DHS. The Office of Intelligence and Analysis' role is to gather information from all field operations and other parts of the Intelligence Community; analyze it for homeland security implications; and appropriately disseminate it to policymakers, DHS components, and federal, state, and local partners. The Office of Intelligence and Analysis is also responsible for coordinating and integrating intelligence-related policies, plans, and procedures, and establishing department-level intelligence requirements.

Our analysis of the Second Stage Review indicated the reorganization recommendations focused on intelligence operations at the department level, and the implementation plan focused on intelligence requirements, collection, analysis and fusion at the strategic level. In addition, the Second Stage Review did not address the blurring definition of "intelligence" within the department. DHS elements that are part of the Intelligence Community detect

² *The Final Report of the National Commission on Terrorist Attacks Upon the United States* (The 9/11 Commission Report), pg. 416.

³ 50 U.S.C. § 401, *et seq.*

and analyze threats to the national security of the United States, while other intelligence organizations in the department collect information and develop analytical products to aid in the capture of prospective or practicing criminals.⁴ Until these activities are differentiated and “intelligence” explicitly defined, the department will face challenges in determining what activities and organizations should be integrated.

The DHS Chief Intelligence Officer has observed that the multiple points of collection in the department reside within DHS component intelligence offices, as well as within the operations of Border Patrol agents, and Custom and Border Protection officers, criminal investigators, airport screeners, and immigration benefits adjudicators. The Office of Intelligence and Analysis developed an overarching vision and strategy for DHS intelligence activities when it released the *DHS Intelligence Enterprise Strategic Plan (Plan)* in January 2006. The Plan defined the DHS Intelligence Enterprise to include all component organizations within the department that have activities producing raw information, intelligence-related information, or finished intelligence.

The Plan signaled a commitment to integrate the intelligence capabilities of the department, but did not specify the component organizations that should be integrated. The Chief Intelligence Officer has testified before Congress that he faces challenges in integrating and coordinating the myriad operational and intelligence-related activities that make up the DHS Intelligence Enterprise.⁵

It is our hope that this survey will assist the Chief Intelligence Officer and other DHS leaders to confront these challenges by providing detailed information about intelligence-related activities in DHS’ field operational units, and identifying several areas where DHS management should take action.

⁴ Departments and agencies cooperating to fulfill the goals of Executive Order 12333 constitute the U.S. Intelligence Community. Executive Order 12333 provides guidelines for the conduct of U.S. intelligence activities.

⁵ Chief Intelligence Officer Charles Allen, *Written Statement to the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment* (October 19, 2005).

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 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.