Department of Homeland Security
Office of Inspector General

Management Oversight and Additional Automated Capabilities Needed to Improve Intelligence Information Sharing

(Redacted)

OIG-11-87

June 2011

Office of Inspector General

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

Homeland Security

June 3, 2011

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 addresses the strengths and weaknesses of the department's capability to share intelligence and threat information among its components. It is based on direct observations and analyses of applicable documents. We obtained additional supporting documentation through interviews with personnel from selected components.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust 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.

Charles K. Edwards
Acting Inspector General

Table of Contents/Abbreviations

Executive Summary 1

Background 2

Results of Audit 4

Actions Taken to Share Intelligence Information 4

Management Oversight is Needed to Improve the Effectiveness of the Intelligence Information Sharing Process 6
Recommendations 10
Management Comments and OIG Analysis 10

[redacted] Capabilities are Needed to Enhance the Consolidation and Dissemination of Intelligence Information 12
Recommendations 16
Management Comments and OIG Analysis 16

Appendices

Appendix A: Purpose, Scope and Methodology 19
Appendix B: Management Comments to the Draft Report 20
Appendix C: Major Contributors to this Report 24
Appendix D: Report Distribution 25

Abbreviations

ATS	Automated Targeting System
CBP	Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
ICE	Immigration and Customs Enforcement
IT	information technology
JWICS	Joint Worldwide Intelligence Communications System
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
TRACE	TSA Remote Access to Classified Enclave
TSA	Transportation Security Administration
USCIS	United States Citizenship and Immigration Services

USCG	United States Coast Guard
USSS	United States Secret Service

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We audited the Department of Homeland Security's (DHS) intelligence information sharing capabilities to assess the processes, information technology (IT) systems, and other mechanisms used by the department and its components to share intelligence and threat information. Our objective was to determine whether DHS has established effective department-wide processes and information systems to share intelligence and threat information.

DHS has taken actions to create an environment and infrastructures necessary to promote intelligence information sharing. Specifically, the Office of Intelligence and Analysis (I&A) is responsible for leading and managing the DHS Intelligence Enterprise and establishing a unified, coordinated, and integrated intelligence program for the department. Additionally, I&A established various councils, boards, and a task force to serve as forums for the components' leadership and offices to collaborate on information sharing initiatives and to address information sharing issues. Further, components are developing intelligence information sharing systems to increase communication with their field offices and other DHS components.

I&A can further improve the department's intelligence information sharing capabilities to ensure that components have the relevant data, policies, and information systems to perform their missions. I&A needs to provide additional management oversight to improve the effectiveness of the intelligence information sharing process. Specifically, I&A needs to finalize its policies and procedures to clarify and promote intelligence information sharing across the department. Additionally, I&A needs to improve intelligence information sharing system capabilities to ensure that threat and vulnerability information is readily available to allow a timely response.

Background

Effective intelligence information sharing is vital to enable DHS to carry out its mission of combating terrorist threats and attacks. The ability to gather, analyze, disseminate, and utilize intelligence information is paramount to our national security. It is imperative that DHS provides maximum access to and dissemination of intelligence information among its components, while balancing the obligation of protecting intelligence sources and methods to meet its overall mission.

In February 2007, the Secretary issued the OneDHS memorandum to establish the policy on internal information sharing and exchange. Additionally, the Under Secretary of Intelligence and Analysis has been designated as the Chief Intelligence Officer for the department. The Under Secretary of Intelligence and Analysis is responsible for leading and managing the DHS Intelligence Enterprise and establishing a unified, coordinated, and integrated intelligence program for the department. To better meet its intelligence information sharing responsibilities, I&A established overarching priorities for its intelligence enterprise:

- Improve the quality of intelligence analysis across the department.
- Integrate DHS intelligence across several components.
- Ensure effective service to all homeland security stakeholders, including all of DHS and the Intelligence Community.[1]

I&A initiated several actions to integrate the department's intelligence enterprise. For example, in 2006, I&A developed the DHS Intelligence Enterprise Strategic Plan, which provides the goals to guide the department in integrating, synchronizing, and advocating for the DHS intelligence mission. The plan was updated in 2008 to further outline DHS' commitment to an integrated common intelligence mission and to strengthen analytical and dissemination capabilities throughout the department.

[1] The Intelligence Community is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary to protect the national security of the United States.

Additionally, Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Secret Service (USSS) have established specific offices to carry out their intelligence gathering and assessment responsibilities. These components serve as the lead on intelligence and analyses related to their specific mission of providing timely and accurate information on threats to transportation, immigration, or border security. The intelligence information is provided to the department's leadership and other components, such as the Federal Emergency Management Agency (FEMA), National Protection and Programs Directorate (NPPD), and United States Citizenship and Immigration Services (USCIS) to ensure that they are notified of and are prepared for potential terrorist threats.

Further, DHS has deployed enterprise-wide information systems, such as the Homeland Security Information Network (HSIN) and Homeland Secure Data Network (HSDN), and has access to the Joint Worldwide Intelligence Communications System (JWICS) to serve as the technical means of sharing intelligence and threat data among components. These systems provide the network and information technology infrastructure that allows DHS personnel to exchange and share all types of intelligence information with stakeholders.

DHS uses JWICS, a Department of Defense system, to transmit information classified as "Top Secret/ Sensitive Compartmented Information." JWICS provides intelligence personnel with access to other Intelligence Community highly secured intelligence systems, intranets, and databases to conduct research and obtain intelligence updates. HSDN is a wide area network, classified as "Secret," for DHS and its components with specific and controlled interconnections to the Intelligence Community and federal law enforcement resources, such as Secret Internet Protocol Router Network.[2] With HSDN, DHS has the ability to collect, disseminate, and exchange both tactical and strategic intelligence information throughout DHS and its partners.

[2] The Secret Internet Protocol Router Network is a system of interconnected computer networks used by the Departments of Defense and State to transmit information classified as "Secret" in a secure environment.

DHS developed HSIN, a web-based platform for sharing and collaborating sensitive but unclassified information among federal agencies, state, local, tribal, private sector, and international partners. HSIN was created to interface with existing information sharing networks to support the diverse communities of interest engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents under the jurisdiction of DHS. Currently, HSIN has more than main communities of interest portals.

Results of Audit

Actions Taken To Share Intelligence Information

DHS has taken actions to create an environment and infrastructures necessary to promote intelligence information sharing in support of its mission. For example, DHS has established forums that make up the governance structure to share intelligence information. Some of the actions designed to foster and improve intelligence information sharing among the components include:

- Established the Information Sharing Governance Board, Homeland Security Intelligence Council, and Information Sharing Coordination Councils to serve as forums for executives, key intelligence officials, and program managers to coordinate the exchange of intelligence information within the department and make sound operational decisions.

- Established the DHS Threat Task Force to coordinate a comprehensive DHS response to potential homeland security incidents. It adds value by integrating component data early in the analytical process and enhances intelligence reporting and information sharing across the components.

- Collaborated with the Intelligence Community and DHS components on emergent threats and improved situational awareness through the use of secure video teleconferences.

Additionally, components are developing their intelligence information sharing systems to increase communication among their field offices, offsite personnel, and other DHS components, as well as their external partners. Components with similar intelligence and law enforcement

missions exchange relevant information that is captured in their component-specific information systems. Some component-specific initiatives include:

- USCG has established an agreement to use the information captured in CBP's Automated Targeting System (ATS) to perform its intelligence mission.[3] Both components have extended the functionality of ATS to include USCG data that both components can use to facilitate a better environment to exchange information.

- CBP is developing and testing its Analytical Framework for Intelligence system to increase its data consolidation and analyses and enhance collaboration and information sharing between analysts. It also facilitates and consolidates access to existing CBP data sources.

- I&A is developing the to provide .

- TSA is adding a new capability to its TSA Remote Access to Classified Enclaves (TRACE) system .

- USCIS is developing and testing its Citizenship and Immigration Data Repository, which allows intelligence analysts to conduct person-centric data analyses using USCIS datasets and classified data sources. The systems also facilitate requests for information received from other agencies.

While actions have been taken to facilitate the exchange of intelligence information within the department, I&A still faces numerous challenges in carrying out its mission as the leader of the Homeland Security Intelligence Community and a provider of high-quality analysis. I&A

[3] CBP uses ATS to improve the collection, use, analysis, and dissemination of information to target, identify, and prevent potential terrorists and terrorist weapons from entering the United States and identify other violations and violators of United State laws. ATS enables CBP officers to focus their efforts on travelers and cargo shipments that most warrant further attention.

must continue to improve in performing its intelligence functions: collecting, analyzing, sharing, and managing intelligence data. Additionally, I&A must encourage components to share their systems and capabilities so that the department can keep abreast of new developments and respond to terrorist attacks.

Management Oversight is Needed to Improve the Effectiveness of the Intelligence Information Sharing Process

I&A is hindered in its ability to provide an effective intelligence and information sharing program for the department. Specifically, I&A needs to strengthen its oversight and better leverage component intelligence activities and initiatives to establish a unified department intelligence mission. Additionally, I&A has not finalized various policies and procedures to clarify and promote intelligence information sharing across the department. Without a unified intelligence mission and policies, DHS will continue to maintain a fragmented and less than optimal intelligence enterprise.

DHS' Intelligence Activities are Not Integrated

DHS intelligence activities are fragmented, hindering I&A's ability to promote effective intelligence information sharing across the department. This is occurring, in part, because I&A has not provided sufficient oversight of component intelligence organizations in order to leverage their respective activities. Specifically, I&A has not implemented intelligence activities and initiatives on an enterprise level. As a result, components are constantly developing systems for their specific mission and intelligence needs. Without I&A's oversight, components will continue to operate independently in their intelligence activities and initiatives and will not be able to provide the department with a more efficient and effective intelligence function.

Although components look to I&A for guidance and coordination of intelligence activities and information, some components expressed concern that I&A is not performing its intelligence analysis more efficiently to ensure that their initiatives are implemented in a timely manner. Additionally, components view I&A as the focal point for disseminating homeland security intelligence for the department. Since I&A has direct access to the Intelligence Community, it has access to intelligence information

that other components do not have. Components' intelligence analysts believe that they could use the additional intelligence information from I&A to improve their analyses to make informed decisions concerning potential terrorist threats.

Further, component intelligence officials told us they prefer to have I&A's guidance when developing their intelligence activities initiatives. For example, I&A can assist them during various phases of the initiatives, on legal, privacy, and civil liberties issues. Further, I&A can assist in determining whether additional rules or data sets can be incorporated to expand the purpose and functionalities of existing or newly developed systems.

According to the *Homeland Security Act of 2002*, as amended, DHS is the focal point for preventing and responding to terrorist attacks and other emergencies. *Homeland Security Presidential Directive – 5* requires DHS to coordinate federal operations to prepare for, respond to, and recover from terrorist attacks and other emergencies. Further, the *National Response Framework* emphasizes that DHS is the primary national hub for situational awareness and operations coordination across the federal government for incident management, in providing the Secretary with intelligence and information necessary to make critical national level decisions.

By increasing its oversight functions, I&A will be in a stronger position to leverage component-specific intelligence activities and initiatives to ensure that the benefits can be shared on an enterprise level to achieve potential cost savings. Also, component intelligence analysts will have additional information available from I&A to better perform their duties. Further, I&A can make certain, to the extent possible, that new and existing information systems are compatible with one another. Therefore, by fostering an integrated homeland security approach to intelligence and strengthening assistance to maximize intelligence collaboration, I&A can advance partnerships among the components.

Overarching and Specific Operational Intelligence Information Sharing Policies and Procedures Are Needed

DHS does not have overarching and operational policies and procedures that specifically address intelligence information sharing. For example, the DHS Information Sharing Strategy and the DHS Intelligence Enterprise Strategic Plan do not provide

detailed guidance to components on how to share intelligence information. Although both documents emphasize the need to foster communication between law enforcement agencies and the Intelligence Community, they do not contain a comprehensive method to share intelligence information that the components can implement. Although DHS stresses the need to establish a uniform, single information sharing environment, components' intelligence officials informed us that they are still unclear as to what they can share with other components, as current strategies are too broad.

The *Homeland Security Act of 2002*, as amended, requires DHS to disseminate, as appropriate, information analyzed within the department and other agencies to assist in the deterrence, prevention, preemption of, or response to terrorist attacks. Additionally, the *Intelligence Reform and Terrorism Prevention Act of 2004*, as amended, requires the Information Sharing Environment, in which DHS participates, to facilitate the availability of terrorism information in a form and manner that facilitates its use in analysis, investigations, and operations.

I&A acknowledges the need to develop policies and procedures for intelligence information sharing. Currently, I&A is revising DHS Management Directive 8110, *Intelligence Integration and Management*, to delineate the policies and related responsibilities needed to develop and strengthen an integrated and collaborative DHS Intelligence Enterprise. Also, I&A is developing the Homeland Security Intelligence Priorities Framework to establish a department-wide method for identifying and prioritizing intelligence that supports the department's operations. The framework would enable department leadership to align DHS' intelligence activities with I&A's priorities to identify shortages, redundancies, and opportunities for collaboration.

Further, I&A needs to leverage knowledge obtained from information sharing assessments to develop specific operational policies and procedures. For example, I&A performed an information sharing assessment of the Southwest Border to better understand the needs and limitations of border operations.[4] The premise of this assessment was to develop the strategic vision and

[4] *Department of Homeland Security Intelligence and Analysis: Southwest Border Information Sharing Assessment*, January 2010.

policies to characterize individual processes, activities, and interactions of the organization.

. Until these assessments are completed, I&A cannot .

See Figure 1 for the full listing of DHS mission areas.

Mission 1: Preventing Terrorism and Enhancing Security
Goal 1.1: Prevent Terrorist Attacks
Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities
Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events
Mission 2: Securing and Managing Our Borders
Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders
Goal 2.2: Safeguard Lawful Trade and Travel
Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations
Mission 3: Enforcing and Administering Our Immigration Laws
Goal 3.1: Strengthen and Effectively Administer the Immigration System
Goal 3.2: Prevent Unlawful Immigration
Mission 4: Safeguarding and Securing Cyberspace
Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment
Goal 4.2: Promote Cybersecurity Knowledge and Innovation
Mission 5: Ensuring Resilience to Disasters
Goal 5.1: Mitigate Hazards
Goal 5.2: Enhance Preparedness
Goal 5.3: Ensure Effective Emergency Response
Goal 5.4: Rapidly Recover

Figure 1: DHS Homeland Security Missions

Although these efforts attempt to address intelligence information sharing needs, they are limited to a specific level or mission area. For example, while Management Directive 8110 describes broad responsibilities at the managerial level, it does not allocate intelligence information sharing responsibilities at the operational level. Without [redacted] to potential threats to the homeland. By issuing detailed intelligence information sharing policies and procedures, I&A can establish a common standard to ensure that relevant and time-sensitive information is available to components.

Recommendations

We recommend that the Under Secretary for Intelligence and Analysis:

Recommendation #1: Develop and implement an [redacted] of intelligence information across the department. The policy should (1) delineate I&A's roles and responsibilities as the leader of DHS' intelligence enterprise, and (2) require components to develop [redacted] intelligence information throughout the department.

Recommendation #2: Coordinate with component Chief Information Officers on intelligence system initiatives to achieve [redacted] of systems.

Recommendation #3: Perform intelligence information sharing assessments in the other mission areas to identify areas of improvement and develop operational policies and procedures to address deficiencies.

Management Comments and OIG Analysis

I&A concurred with recommendation 1. I&A has been engaged in the approval process for Management Directive 213, an updated version of *Intelligence Integration and Management* (formerly Management Directive 8110). Once approved by the department,

Management Directive 213 should provide DHS and its components with a reliable basis for understanding the roles of I&A and the DHS Chief Intelligence Officer, as well as enabling the Chief Intelligence Officer to manage components' efforts to identify relevant data and develop robust mechanisms for sharing intelligence information.

We agree that the steps I&A has taken, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until I&A provides documentation to support that all planned corrective actions are completed.

I&A concurred with recommendation 2. I&A actively engages in efforts to intelligence systems through the National Security Systems Board and the Chief Information Officers Council. The completion of these efforts will help to drive the maturation of the Intelligence Enterprise and to encourage the unimpeded flow of intelligence information throughout the department.

We agree that the steps I&A has taken, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until I&A provides documentation to support specific efforts taken to intelligence systems throughout the department.

I&A concurred with recommendation 3. The Information Sharing and Intelligence Enterprise Management Division within I&A has initiated a project to develop information sharing diagrams for selected flows within the major information sharing mission areas. These flow diagrams, when completed, will identify areas of needed improvement and will enable the Chief Intelligence Officer and components to develop functional standards and information exchange protocols to all for increased automated sharing.

We agree that the steps I&A has taken, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until I&A provides documentation to support that all planned corrective actions are completed.

Capabilities are Needed to Enhance the Consolidation and Dissemination of Intelligence Information

DHS does not have Additionally, DHS needs to improve the functionality and interoperability of its existing intelligence systems at components to promote better collaboration within the department. Also, DHS needs to develop a component intelligence analysts will continue to face hurdles when researching and sharing intelligence information.

Components' Abilities to Share

The department has to all the intelligence analysts. Further, DHS does of intelligence information.

I&A encourages the components to use HSDN to share intelligence analysis and information. Some components' intelligence officials stated that they and that HSDN and HSIN system constraints limit their effectiveness. For example, CBP, ICE, and USSS personnel informed us that many of their . Also, HSDN is . According to a CBP official, a field agent may Some CBP agents have to

ICE personnel informed us that to exchange intelligence information.

Component officials and intelligence analysts identified a number of constraints that limit HSDN's effectiveness:

Similar to HSDN, HSIN has a number of constraints that limit its effectiveness. However, component personnel noted a number of concerns regarding HSIN:

The *Homeland Security Act of 2002*, as amended, requires DHS to establish appropriate systems, mechanisms, and procedures to share threat and vulnerabilities information that is relevant to national critical infrastructure and key resources with other federal agencies, state and local governments, and the private sector in a timely manner. Additionally, the Under Secretary of Intelligence and Analysis is required to establish and utilize, in conjunction with the department's Chief Information Officer, a secure communications and information technology infrastructure. The infrastructure should include other advanced analytical tools to access, receive, and analyze data and information and to disseminate information acquired and analyzed by the department. Further, the *National Response Framework* requires that coordinating mechanisms be provided for expedited and proactive federal support to ensure that critical life-saving assistance and incident containment capabilities are in place for a quick and efficient response to catastrophic incidents.[5]

Additionally, intelligence analysts do not These concerns will continue to hinder analysts' abilities to perform their duties and impact the quality, efficiency, and effectiveness of intelligence information sharing.

is Needed to Perform Searches of Intelligence Information on

DHS does not have an of intelligence information Specifically, component intelligence analysts have to for law enforcement and intelligence information.

[5] The *National Response Framework* highlights improvements to the previous *National Response Plan*. The *Framework* superseded the *Plan*, which focused largely on federal roles and responsibilities.

[6] search query.

[redacted]

[redacted] For example, the ICE Law Enforcement Information Sharing service will be the first [redacted] DHS is looking for ways to accelerate the implementation at or shortly after the initial operating capability that is scheduled for September 2011.

With [redacted] analyze and warn of potential terrorist threats more effectively.

A [redacted] Can Share Intelligence Products More Effectively

DHS needs to improve its intelligence information sharing and collaboration efforts among the components to ensure that threats and incidents are mitigated timely. Specifically, DHS needs to provide an [redacted] can be shared.

[redacted]

I&A is aware of some of the components' concerns regarding In response, I&A has developed several proposed enhancements on its including implementing .[7] For example, I&A plans to have in the near future.

Recommendations

We recommend that the Under Secretary of Intelligence and Analysis collaborate with the DHS CIO, to:

Recommendation #4: Develop a products.

Recommendation #5: Acquire technology to

Management Comments and OIG Analysis

I&A concurred with recommendation 4. I&A has partnered with CBP to bring the collaborative capabilities This effort seeks to expand DHS' ability to connect people and to facilitate information sharing.

[7]

[redacted]

[redacted]

We agree that the steps that I&A has taken, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until I&A provides documentation to support that all planned corrective actions are completed.

I&A concurred with recommendation 5. [redacted]

[redacted]

[redacted]

We agree that the steps that I&A has taken, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until I&A provides documentation to support that all planned corrective actions are completed.

Appendix A
Purpose, Scope, and Methodology

The objective of our audit was to determine whether DHS has established a department-wide capability to effectively share intelligence and threat information. Specifically, we determined whether DHS has established a standardized process to share intelligence and threat information.

Our review focused on DHS' intelligence sharing activities based on the requirements outlined in *The Homeland Security Act* (2002), *The Intelligence Reform and Terrorism Prevention Act* (2004), Executive Orders 12333 (1981) and 13356 (2004), the *DHS Intelligence Enterprise Strategic Plan* (2008), the *DHS Information Sharing Strategy* (2008), and the *National Strategy for Information Sharing* (2007). We interviewed selected DHS management and intelligence officials, as well as officials from the National Operations Center. Further, we interviewed personnel from CBP, FEMA, ICE, I&A, NPPD, TSA, USCG, USCIS, and USSS regarding DHS' communication methods, systems inventory, technologies, tools, and arrangements that the components use to collect, analyze, and disseminate intelligence information. We did not evaluate the effectiveness of security controls implemented for the intelligence systems. Additionally, we did not evaluate fusion centers, state and local entities, and their associated intelligence systems.

We conducted this performance audit between August 2010 and February 2011 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. Major OIG contributors to the audit are identified in Appendix C.

The principal OIG point of contact for the audit is Frank W. Deffer, Assistant Inspector General, IT Audits, at (202) 254-4100.

Appendix B
Management Comments to the Draft Report

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

Homeland Security

Frank W. Deffer
Assistant Inspector General, IT Audits
DHS Office of Inspector General
1120 Vermont Avenue Northwest
Washington, DC 20005

Dear Mr. Deffer:

RE: Draft Report OIG-10-028-ITA-DHS, *Management Oversight and Additional Automated Capabilities Needed to Improve Intelligence Information Sharing*

The Department of Homeland Security appreciates the opportunity to review and comment on the draft report referenced above. The Department, particularly the Office of Intelligence and Analysis, concurs with the recommendations in the report.

We acknowledge the collaboration that your staff has undertaken with our program managers and liaisons to adjust the language of these recommendations. We also appreciate the effort that your staff has made to ensure the proper assignment and direction of the report's recommendations, as it will do much to assist us with their implementation.

While much progress has been made to improve intelligence information sharing throughout the Department, including efforts at the National Security Systems Board and the Chief Information Officers Council, we agree that much work remains to be done. A number of documents are in the process of Departmental clearance that, when final, will provide greater clarity and efficiency in the sharing of intelligence information. We will also work closely with your staff to ensure that this report's recommendations are suitably addressed and executed.

Again, we appreciate this opportunity to review and comment on the draft report. In addition to this response, technical comments and a sensitivity review were provided under separate cover.

Sincerely,

Caryn A. Wagner
Under Secretary for Intelligence
and Analysis

Appendix B
Management Comments to the Draft Report

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

Homeland Security

13 April 2011

Frank W. Deffer
Assistant Inspector General, IT Audits
DHS Office of Inspector General
1120 Vermont Avenue Northwest
Washington, D.C. 20005

Dear Mr. Deffer:

RE: Draft Report OIG-10-028-ITA-DHS, *Management Oversight and Additional Automated Capabilities Needed to Improve Intelligence Information Sharing*

The Department of Homeland Security (Department/DHS), particularly the Office of Intelligence and Analysis (I&A), appreciates the opportunity to review the draft report referenced above and to provide corrective actions that are germane to the report recommendations as listed below.

We recommend that the Under Secretary for Intelligence and Analysis:

Recommendation: Develop and implement an [redacted] of intelligence information across the Department. The policy should (1) delineate I&A's roles and responsibilities as the leader of DHS' Intelligence Enterprise, and (2) require components to develop [redacted] intelligence information throughout the Department.

Response: Concur. The Office of Intelligence & Analysis has been engaged in the approval process for MD 213, an updated version of *Intelligence Integration and Management* (MD 8110). Once approved by the Department, MD 213 should provide DHS and its components with a reliable basis for understanding the roles of I&A and the DHS Chief Intelligence Officer (CINT) and enable the CINT to manage components' efforts to identify relevant data and develop robust mechanisms for sharing intelligence information.

Recommendation: Coordinate with component Chief Information Officers on intelligence system initiatives to achieve [redacted] of systems.

Response: Concur. As mentioned in the letter from the Under Secretary, I&A actively engages in efforts to [redacted] intelligence systems through the National Security Systems Board and the Chief Information Officers Council. The completion of these efforts will help to drive the maturation of the Intelligence Enterprise and to encourage the unimpeded flow of intelligence information throughout the Department.

Recommendation: Perform intelligence information sharing assessments in the other mission areas to identify areas of improvement and develop operational policies and procedures to address deficiencies.

Response: Concur. The Information Sharing and Intelligence Enterprise Management Division (ISIEM) within I&A has initiated a project to develop information sharing flow diagrams for selected flows within the major information sharing mission areas. These flow diagrams, when completed, will identify areas of needed improvement and will enable the CINT and components to develop functional standards and information exchange protocols to all for increased automated sharing.

We recommend that the Under Secretary for Intelligence and Analysis collaborate with the DHS CIO to:

Recommendation: Develop a [redacted] products.

Response: Concur. I&A has partnered with U.S. Customs and Border Protection (CBP) to bring the collaborative capabilities [redacted]. This effort seeks to expand DHS's ability to connect people and to facilitate information sharing.

[redacted]

[redacted]

Recommendation: Acquire technology to [redacted]

Response: Concur. [redacted]

[redacted]

[redacted]

Again, we appreciate this opportunity to review and comment on the draft report and to provide corrective actions to the recommendations. Unfortunately, due to the extensive effort and collaboration required for the above mentioned corrective action plans, we are unable to provide precise completion dates for them, although we can assert that timelines for each will likely exceed 90 days. In addition to this response, technical comments and a sensitivity review have been provided under separate cover.

Sincerely,

Todd M. Rosenblum
Senior Component Accountable Official
Office of Intelligence and Analysis

Appendix C
Major Contributors to this Report

Information Security Audit Division

Chiu-Tong Tsang, Director
Tarsha Cary, Audit Manager
Shannon Frenyea, Senior Program Analyst
Thomas Rohrback, IT Specialist
David Bunning, IT Specialist

Anthony Nicholson, Referencer

Department of Homeland Security

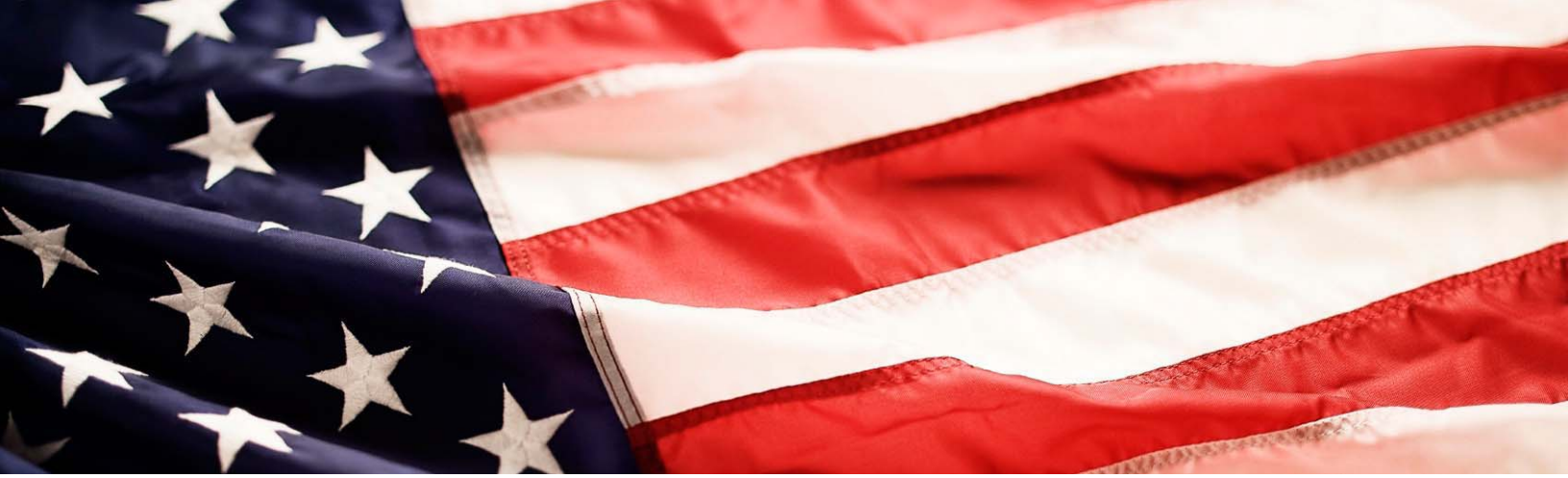
Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary, Office of Intelligence and Analysis (I&A)
Chief Information Officer (CIO)
Deputy CIO
Chief Information Security Officer (CISO)
Director, Compliance and Oversight Program
Director, Knowledge Management Division, I&A
Director, Information Sharing and Intelligence Enterprise Management Division
Audit Liaison, I&A
Audit Liaison, DHS/CISO
Audit Liaison, DHS/CIO
Audit Liaison, CBP
Audit Liaison, FEMA
Audit Liaison, ICE
Audit Liaison, NPPD
Audit Liaison, Operations
Audit Liaison, TSA
Audit Liaison, USCG
Audit Liaison, USCIS
Audit Liaison, USSS

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, 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.