Congressional Research Service
Informing the legislative debate since 1914

The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress

Updated March 19, 2010

Congressional Research Service
https://crsreports.congress.gov
R40602

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The primary mission of the Department of Homeland Security (DHS, the Department) is to "prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, and minimize the damage, and assist in the recovery from terrorist attacks that do occur in the United States." Since its inception in 2003, DHS has had an intelligence component to support this mission and has been a member of the U.S. Intelligence Community (IC).

Following a major reorganization of the DHS (called the Second Stage Review or "2SR") in July 2005, former Secretary of Homeland Security, Michael Chertoff established a strengthened Office of Intelligence and Analysis (I&A) and made the Assistant Secretary for Information Analysis (now Under Secretary for Intelligence and Analysis) the Chief Intelligence Officer for the Department. He also tasked I&A with ensuring that intelligence is coordinated, fused, and analyzed within the Department to provide a common operational picture; provide a primary connection between DHS and the IC as a whole; and to act as a primary source of information for state, local and private sector partners.

Today, the DHS Intelligence Enterprise (DHS IE) consists of I&A, two headquarters elements supported by I&A, and the intelligence elements of six DHS operational components: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE). U.S. Citizenship and Immigration Services (USCIS), the Transportation Security Administration (TSA), U.S. Coast Guard (USCG), and U.S. Secret Service (USSS).

Congress made information sharing a top priority of the Department's intelligence component in the Homeland Security Act of 2002 and underscored its importance through the Intelligence Reform and Terrorism Prevention Act of 2004. Since the 2SR reorganization, Congress imposed additional requirements for intelligence analysis; information sharing; department-wide intelligence integration; and support to state, local, tribal governments, and the private sector through the Implementing Recommendations of the 9/11 Commission Act of 2007.

On February 11, 2010, the Senate confirmed President Obama's selection of Caryn Wagner to serve as Under Secretary for Intelligence and Analysis. As she assumes responsibility for the DHS IE, Congress will likely be interested in the progress of integration of the Department's intelligence components and the quality and relevance of the intelligence DHS IE produces for front line law enforcement and security officials who are responsible for protecting America and its people. In February, DHS produced its first Quadrennial Homeland Security Review (QHSR), a comprehensive assessment outlining its long-term strategy and priorities for homeland security and guidance on the Department's programs, assets, capabilities, budget, policies, and authorities. The next step in the Department's QHSR process is to conduct a "bottom-up review" to systematically link strategy to program to budget. The results of that review will be particularly important as Congress considers an authorization bill for DHS.

This report provides an overview of the DHS IE both at headquarters and within the components. It examines how DHS IE is organized and supports key departmental activities to include homeland security analysis and threat warning; border security; critical infrastructure protection; support to, and the sharing of information with, state, local, tribal, and private sector partners. It also discusses several oversight challenges and options for Congress to consider on these issues. This report may be updated.

Contents

Figures

Contacts

Introduction

A primary mission of the Department of Homeland Security (DHS, Department) is to "prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, and minimize the damage, and assist in the recovery from terrorist attacks that do occur in the United States.[1] The current organization of the Department is displayed at **Figure 1**.

To support this mission, DHS has had an intelligence component since its inception in 2003. The Homeland Security Act of 2002, assigned the original DHS intelligence component—the Directorate of Information Analysis and Infrastructure Protection—with responsibility to receive, analyze, and integrate law enforcement and intelligence information in order to— "(A) identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities of the homeland."[2]

Congress also made information sharing a top priority of the new DHS intelligence organization, requiring it "to disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal government with responsibilities related to homeland security, and to agencies of State and local government and private sector entities, with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States."[3]

Following the release of the *9/11 Commission Report* in 2004, which identified a breakdown in information sharing as a key factor contributing to the failure to prevent the September 11, 2001 attacks,[4] Congress underscored the importance it attached to information sharing at all levels of government. The Intelligence Reform and Terrorism Prevention Act of 2004[5] required the President to "create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties,"[6] and "to designate an individual as the program manager responsible for information sharing across the Federal Government."[7]

In July 2005, following "a systematic evaluation of the Department's operations, policies and structures"[8] (commonly called the Second Stage Review or "2SR"), former Secretary of Homeland Security, Michael Chertoff, initiated a major reorganization of DHS. In his remarks describing the reorganization, he noted that "…intelligence lies at the heart of everything that we do."[9] In an effort to improve how DHS manages its intelligence and information sharing responsibilities, he established a strengthened Office of Intelligence and Analysis (I&A) and made the Assistant Secretary for Information Analysis (now Under Secretary for Intelligence and

[1] P.L. 107-296, Nov. 25, 2002, §101b(1), 116 STAT. 2142.

[2] Ibid., §201d(9), 116 STAT. 2147.

[3] Ibid., §201d(1), 116 STAT. 2146.

[4] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, July 22, 2004, pp. 353-356 and 416-418. http://www.9-11commission.gov. Hereafter: *9/11 Commission Report.*

[5] P.L. 108-458, Dec. 17, 2004.

[6] Ibid, §1016b(1), 118 STAT. 3665.

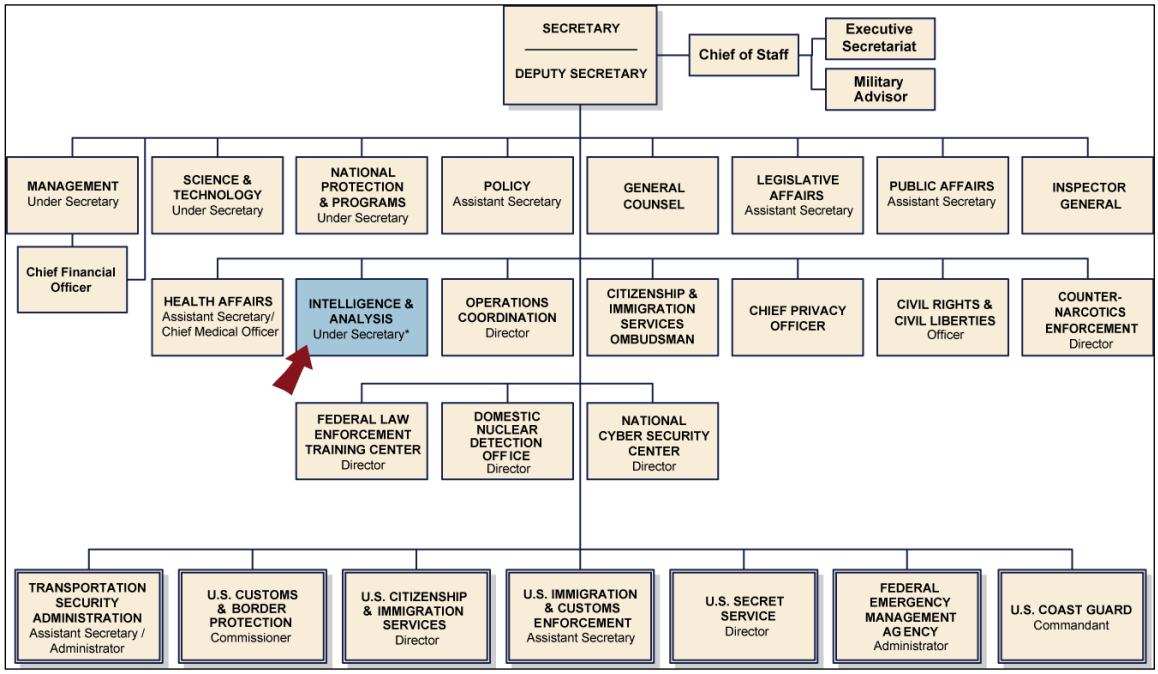
[7] Ibid, §1016f(1), 118 STAT. 3667. The Program Manager-Information Sharing Environment (PM-ISE), is functionally aligned within the Office of the Director of National Intelligence (ODNI).

[8] DHS, "Secretary Michael Chertoff U.S. DHS Second Stage Review Remarks," press release, July 13, 2005. http://www.dhs.gov/xnews/speeches/speech_0255.shtm. Hereafter: Chertoff, "DHS Second Stage Review Remarks."

[9] Ibid.

Analysis) the Chief Intelligence Officer (CINT) for the Department. He also tasked I&A with ensuring that intelligence is coordinated, fused, and analyzed within the Department to provide a common operational picture; provide a primary connection between DHS and the Intelligence Community (IC) as a whole; and to act as a primary source of information for state, local and private sector partners. [10]

Figure 1. Current Department of Homeland Security Organization



Source: DHS, July 18, 2008.

In testimony to a House of Representatives hearing shortly after his selection, the first DHS CINT, stated that "[m]y goal and my role as chief intelligence officer is to see that Homeland Security intelligence, a blend of traditional and nontraditional intelligence that produces unique and actionable insights, takes its place along the other kinds of intelligence as an indispensable tool for securing the nation.[11]

He also set five priorities: Improving the quality of intelligence analysis across the department; integrating the DHS IE; strengthening support to state, local, and tribal authorities and the private sector; ensuring that DHS IE takes its place in the IC; and solidifying the relationship with the Congress; and improving transparency and responsiveness.[12]

[10] Ibid.

[11] U.S. Congress, Joint Hearing of the Intelligence, Information Sharing, and Risk Assessment Subcommittee of the House Committee on Homeland Security and the Terrorism, Human Intelligence, Analysis, and Counterintelligence Subcommittee of the House Permanent Select Committee on Intelligence, "DHS Second Stage Review: The Role of the Chief Intelligence Officer," Testimony of Charles Allen, DHS Chief Intelligence Officer, 109th Cong., 2nd sess., October 19, 2005. Hereafter: Allen Testimony, Oct. 19, 2005.

[12] Ibid.

Since the 2SR reorganization, Congress imposed additional requirements on DHS through the Implementing Recommendations of the 9/11 Commission Act of 2007:[13]

- Integrate information and standardize the format of intelligence products produced within DHS and its components.[14]
- Establish department-wide procedures for review and analysis of information provided by state, local, tribal, and private sector elements; integrate that information into DHS intelligence products, and disseminate to Federal partners within the Intelligence Community.[15]
- Evaluate how DHS components are utilizing homeland security information and participating in the Information Sharing Environment.[16]
- Establish a comprehensive information technology network architecture to connect various DHS elements and promote information sharing.[17]
- Establish a DHS State, Local, and Regional Fusion Center Initiative to establish partnerships with state, local, and regional fusion centers.[18]
- Coordinate and oversee the creation of an Interagency Threat Assessment and Coordination Group that will bring state, local, and tribal law enforcement and intelligence analysts "to work in the National Counterterrorism Center (NCTC)[19] with Federal intelligence analysts for the purpose of integrating, analyzing and assisting in the dissemination of federally-coordinated information…."[20]

The DHS IE consists of those elements within DHS that have an intelligence mission. These include I&A, the Homeland Infrastructure Threat and Risk Analysis Center, and the Intelligence Division of the Office of Operations Coordination and Planning (all located at the DHS headquarters), and the intelligence elements of six operational components: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Transportation Security Administration (TSA), U.S. Coast Guard (USCG), and U.S. Secret Service (USSS). The Department and USCG are statutory members of the IC. [21]

[13] P.L. 110-53, Aug. 3, 2007.

[14] Ibid, §204a, 121 STAT. 307.

[15] Ibid, §204(c)(1)A, 121 STAT. 307.

[16] Ibid, §204(d)(2)A, 121 STAT. 308.

[17] Ibid, §205a, 121 STAT. 308.

[18] Ibid, §511, 121 STAT. 317-18.

[19] NCTC was established by Executive Order (E.O.) 13354 in Aug. 2004, and codified in Section 1021 of the *Intelligence Reform and Terrorism Prevention Act of 2004*. It is the primary U.S. Government organization for integrating and analyzing all intelligence pertaining to counterterrorism (except for information pertaining exclusively to domestic terrorism). Through its Directorate of Strategic Operational Planning, it is also the executive branch lead for counterterrorism planning. See NCTC, *About the National Counterterrorism Center*. http://www.nctc.gov/about_us/about_nctc.html

[20] P.L. 110-53, §521, 121 STAT. 328.

[21] There are 16 statutory members of the IC: the Departments of Energy, Justice (Drug Enforcement Administration), Homeland Security, State, and Treasury; the Central Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency; and the intelligence components of the U.S. Army, Navy, Marines, Air Force, and Coast Guard. See 50 U.S.C. 401a(4)(k).

On February 11, 2010, the Senate confirmed President Obama's selection of Caryn Wagner to serve as Under Secretary for Intelligence and Analysis. As she assumes responsibility for the DHS IE, Congress will likely be interested in the progress of integration of the Department's intelligence components and the quality and relevance of the intelligence DHS IE produces for front line law enforcement and security officials who are responsible for protecting America and its people.

Also in February, DHS published its first Quadrennial Homeland Security Review (QHSR),[22] a comprehensive assessment outlining its long-term strategy and priorities for homeland security and guidance on the Department's programs, assets, capabilities, budget, policies, and authorities. The next step in the Department's QHSR process is to conduct a "bottom-up review" to systematically link strategy to program to budget. The results of that review will be particularly important as Congress considers an authorization bill for DHS.

Some have argued that there is a broad homeland security intelligence enterprise that encompasses not only the DHS IE, but other organizations at the Federal, state, local, tribal, and private sector levels that collect and analyze homeland security information and disseminate intelligence products. This report will focus on the DHS IE both at headquarters and within the components; how it is organized; and how it supports key departmental activities to include homeland security analysis and threat warning, border security, critical infrastructure protection, and support to and the sharing of information with state, local, tribal, and private sector partners. It will also discuss oversight challenges and options for Congress to consider on these issues.

Office of Intelligence and Analysis (I&A)

The Homeland Security Intelligence Mission

According to its December 2009 *Strategy*, the mission of I&A is "To strengthen DHS and its partners' ability to perform homeland security functions by accessing, integrating, analyzing, and sharing timely and relevant intelligence and information, while protecting the privacy, civil rights, and civil liberties of the people I&A serves.[23] It accomplishes this by ensuring that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security customers in the Department, at state, local, and tribal levels, in the private sector, and in the IC."[24] The Under Secretary for I&A is the Chief Intelligence Officer for the Department and is responsible to lead I&A and the entire DHS IE. The Under Secretary is also the Department's chief information sharing officer and is responsible for implementing the objectives of the PM-ISE within DHS.[25]

To accomplish its mission, I&A participates in all aspects of the intelligence cycle" – the process by which information is acquired, converted into finished intelligence, and made available to policymakers. Generally the cycle comprises five steps: planning and direction, collection, processing, analysis, and production and dissemination."[26] It is an iterative process in which

[22] DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland,* February 2010. Available at http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf. Hereafter: DHS *QHSR Report.*

[23] *DHS Office of Intelligence and Analysis Strategy,* Dec. 2009. Hereafter: *I&A Strategy*, Dec. 2009.

[24] DHS, *Office of Intelligence and Analysis.* http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm.

[25] Office of Management and Budget, *Budget of the United States Government: Fiscal Year 2010,* (Washington, DC: U.S. Government Printing Office, 2009), p. 507. Hereafter: OMB: *USG FY10 Budget*.

[26] Jeffrey T. Richelson, *The U.S. Intelligence Community,* 5th ed, (Boulder, CO: Westview Press, 2008), pp. 3-4.

collection requirements based on national security threats are developed, and intelligence is collected, analyzed, and disseminated to a broad range of consumers.

DHS does not generally engage in traditional foreign intelligence collection activities such as imagery intelligence, signals intelligence, human intelligence, measurement and signatures intelligence, and foreign open source intelligence. [27] But, as former Secretary Chertoff has noted:

> Intelligence, as you know, is not only about spies and satellites. Intelligence is about the thousands and thousands of routine, everyday observations and activities. Surveillance, interactions—each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, gives us a sense of the patterns and the flow that really is at the core of what intelligence analysis is all about....[28]

I&A combines the unique information collected by DHS components as part of their operational activities (e.g., at airports, seaports, and the border) with foreign intelligence from the IC; law enforcement information from Federal, state, local, and tribal sources; private sector data about critical infrastructure and key resources; and information from domestic open sources to develop homeland security intelligence.[29] This encompasses a broad range of homeland security threats. It includes border security information to counter human smuggling and trafficking, cargo data to prevent the introduction of dangerous items, information to protect critical infrastructure against all hazards, information about infectious diseases, and demographic data and other research about 'violent radicalization.'[30]

I&A Customers

The DHS I&A *Strategy* identifies its core customers as the President; Secretary of Homeland Security; DHS Components; State, Local, Tribal, and Private Sector Partners (through State and Major Urban Area Fusion Centers); the IC; and Federal Interagency Partners.[31] In short, I&A's customers range from the Chief Executive all the way to individual border patrol agents, Coast Guard seamen, and airport screeners.

According to Under Secretary Wagner, "A primary role of I&A is to share intelligence and information with our partners at the state, local, tribal, and private sector levels. It is our job to meaningfully convert what may appear to be bits of unrelated information into a product that helps protect our communities."[32] State, local, and tribal law enforcement are "first preventers" of terrorism and require timely and actionable intelligence to respond to threats. They also need intelligence about the latest terrorist tactics and techniques so that they know what to look for and what to do when they encounter suspicious behavior or dangerous items. In addition, I&A

Hereafter: Richelson, *The U.S. Intelligence Community*.

[27] For a detailed description of each of these collection disciplines, see Ibid, chapters 7-12.

[28] Chertoff, "DHS Second Stage Review Remarks."

[29] For a discussion of the concept of homeland security intelligence, see CRS Report RL33616, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, by Mark A. Randol.

[30] Congress has defined 'violent radicalization' as "the process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change." H.R. 1955, *Violent Radicalization and Homegrown Terrorism Prevention Act of 2007,* §899(a)(2).

[31] *I&A Strategy*, Dec. 2009.

[32] U.S. Congress, House Committee on Appropriations, Subcommittee on Homeland Security, *DHS Intelligence Programs and the Effectiveness of State and Local Fusion Centers*, Statement of Caryn Wagner, Under Secretary for Intelligence and Analysis, 111th Cong., 2nd sess., Mar. 4, 2010, p. 3. Hereafter: Wagner Testimony, Mar. 4, 2010.

supports the operators of the nation's publicly and privately-owned critical infrastructure with threat information and other intelligence that supports their risk management decision making.

Former Under Secretary Charles Allen noted that "virtually any terrorist attack on the homeland that one can imagine must exploit a border crossing, a port of entry, a critical infrastructure, or one of the other domains that the department has an obligation to secure. DHS Intelligence must learn and adapt faster than the enemy, so that our department with all its partners in the federal, state, and local levels of government and the private sector have the information edge they need to secure our nation."[33]

I&A is a full partner within the IC and represents DHS on several IC committees. The Under Secretary, for example, is a member of the Director of National Intelligence (DNI)[34] Executive Committee. I&A contributes analytic staff to the National Counterterrorism Center (NCTC). The office also contributes items to the President's Daily Brief[35] providing a unique homeland security perspective on terrorism and other threats to the United States to the nation's leaders.

Integrating the DHS IE

Among the many challenges for DHS since its founding has been the integration of 22 legacy and newly-created agencies. This also includes the integration of intelligence activities of the Department's operational components whose intelligence organizations predate the establishment of DHS. These intelligence elements were created to support the operational missions of their respective components and were tailored accordingly.

One of the objectives of the Department's 2005 2SR reorganization was to enhance integration to include its intelligence effort. The Under Secretary for I&A is also the Chief Intelligence Officer for the entire Department. Congress also made the Under Secretary responsible to "establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department."[36]

Homeland Security Intelligence Council (HSIC)

The heads of the DHS intelligence components do not report to the Under Secretary, but to their respective component chiefs. However, pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007, they are required to advise and coordinate closely with the Under Secretary on their activities in support of the intelligence mission of the Department.[37]

The HSIC was established to serve as the mechanism to provide senior-level direction for Department-wide intelligence activities and to promote integration efforts. It is chaired by the

[33] Allen Testimony, Oct. 19, 2005.

[34] The DNI serves as the head of the IC and is the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security. The position was created by Congress in Section 1011 of the *Intelligence Reform and Terrorism Prevention Act of 2004*. The DNI Executive Committee consists of the heads of the IC member agencies.

[35] The PDB compiles the IC's highest level intelligence analysis targeted at the key national security issues and concerns of the President. It is given only to the President, the Vice President, and a very select group of Cabinet-level officials designated by the President. See CIA, "Directorate of Intelligence Products." https://www.cia.gov/offices-of-cia/intelligence-analysis/products.html

[36] P.L. 110-53, August 3, 2007, §531, 121 STAT. 3332-3. Amends §201 of the *Homeland Security Act of 2002* by adding paragraphs 18 and 19.

[37] Ibid, §503, 121 STAT. 311-2. Amends the *Homeland Security Act of 2002* by adding §207.

Under Secretary and is comprised of the key intelligence officials in applicable DHS components. In March 2010 testimony, Under Secretary Wagner, stated that the HSIC "... now reflects a broader range of DHS activities that require intelligence support" and

> ... is focused on governance-level, enterprise-wide objectives, such as collaboratively defining intelligence activities for the Department's Bottom Up Review; and developing new tools for conducting DHS Intelligence Enterprise program reviews. The HSIC oversaw the completion of the first coordinated, Enterprise-wide analytic production plan, which builds on the expertise of the operational components to produce products in their areas, deconflicts competing efforts, and helps focus analytic efforts on QHSR priorities.[38]

Budget

I&A is funded through the classified National Intelligence Program (NIP), formerly known as the National Foreign Intelligence Program. For budgetary purposes, intelligence spending is divided between the NIP; and the Military Intelligence Program that supports the Secretary of Defense's intelligence- and counterintelligence-related responsibilities.[39] The DNI does not publicly disclose details about the intelligence budget,[40] but consistent with Section 601 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), the DNI reported that the aggregate amount appropriated to the NIP for FY2009 was $49.8 billion.[41]

As part of its responsibility to integrate Department intelligence activities, the Under Secretary for I&A is responsible for presenting a consolidated intelligence budget to the Secretary. DHS operational component intelligence activities are generally not part of the NIP—therefore they are not classified—with the exception of the activities of the Coast Guard's National Intelligence Element.[42] Those budgets are listed within each component's appropriation, however they are generally co-mingled with other operational activities.[43] Within the FY2009 homeland security appropriation, the total I&A budget figure (classified) is combined with the budget figure for operational activities (unclassified) within the Analysis and Operations category.[44]

I&A Organization

I&A is led by an Under Secretary, a position subject to Senate confirmation. The Under Secretary also serves as the department's Chief Intelligence Officer. Caryn Wagner assumed this position on February 11, 2010. The Under Secretary is supported by a Principal Deputy Under Secretary, currently Mr. Bart R. Johnson, who served as Acting Under Secretary from May 2009-February 2010.

---

[38] Wagner Testimony, Mar. 4, 2010, p. 5.

[39] DOD Financial Management Regulation 7000.14_R, June 2007, p. 16-2. http://www.fas.org/irp/agency/dod/finman.pdf.

[40] The bulk of overall intelligence spending is contained within the DOD budget. Spending for most intelligence programs is described in classified annexes to intelligence and national defense authorization and appropriations legislation. All Members of Congress have access to these annexes, but must make special arrangements to read them. See DNI, *The Intelligence Budget Process.* http://www.intelligence.gov/2-business_nfip.shtml

[41] Office of the DNI News Release No. 33-09, "DNI Releases Budget Figure for 2009 National Intelligence Program," Oct. 30, 2009.

[42] For a discussion of the USCG National Intelligence Element, see the USCG section of this report.

[43] See CRS Report R40642, *Homeland Security Department: FY2010 Appropriations*, coordinated by Jennifer E. Lake and Chad C. Haddal.

[44] Ibid, Table 6, p. 10.

The current I&A organization is at **Figure 2.** However to support the strategic goals of its December 2009 *Strategy* and the homeland security missions described in the Department's QHSR report, I&A intends to realign organizationally in 2010.

The Analysis Mission

I&A is focused on five "analytic thrusts" aligned with the principal threats to the Homeland:[45] border security, including narcotics trafficking, alien and human smuggling, and money laundering; radicalization and extremism; particular groups entering the United States that could be exploited by terrorists or criminals; critical infrastructure and key resources; and weapons of mass destruction (WMD) and health threats.

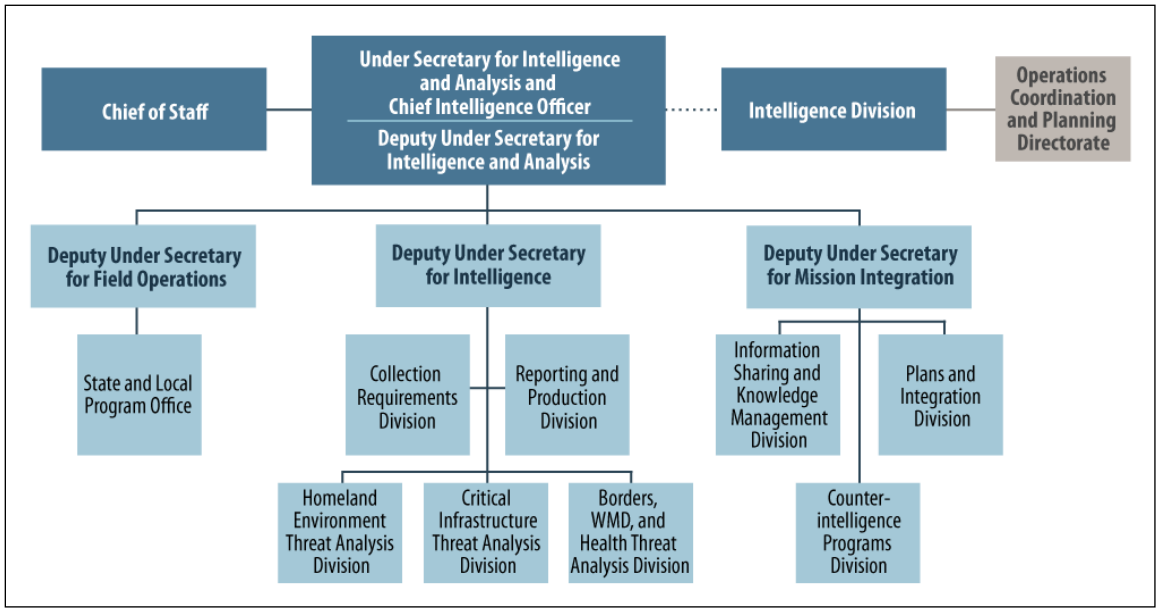
Following a 2009 comprehensive evaluation of its analytic capabilities and functions, I&A has informed Congress that its analysis and production resources have been prioritized to:

- Realign analytic resources to improve and expand support to [the] state, local, and tribal consumer base.
- Develop an analytic capability and methodology for assessing Suspicious Activity Reporting data.
- Create a centralized analysis group to meet the intelligence and information needs of the Secretary and Department components, including improved coordination and information sharing.
- Augment [the] border security analytic capability.
- Strengthen our collaboration and consultation with other producers of intelligence and information products.[46]

[45] DHS I&A, "Homeland Security Analytic Priorities." http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm

[46] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *I&A Reconceived: Defining a Homeland Security Intelligence Role*, Statement of Bart. R. Johnson, Acting Under Secretary for Intelligence and Analysis, 111th Cong., 1st sess., Sep. 24, 2009, pp. 7-8. Hereafter: Johnson Testimony, Sep. 24, 2009.

Figure 2. Office of Intelligence and Analysis Organizational Chart



Source: DHS I&A, March 2009.

I&A Intelligence Products

I&A produces numerous products for its customers. In 2008, there was a realignment and standardization of the I&A finished intelligence product line which now include:

- *Homeland Security Threat Assessment (HSTA)*. This is an annual threat assessment that represents the analytical judgments of DHS and assesses the major threats to the homeland for which the nation must prepare and respond. This includes the actions, capabilities, and intentions of domestic and foreign terrorists and extremists and the possible occurrence of systemic threats. It focuses on domestic extremists, international terrorists operating in the homeland or directing attacks against it, and systemic threats such as pandemics and transnational criminal organizations.[47] The HSTA is produced in classified and "Unclassified/For Official Use Only" versions.
- *Intelligence Warning.* Contains urgent intelligence.
- *Intelligence Note.* Contains timely information or analysis on a current topic.
- *Homeland Security Assessment.* Consists of in-depth analysis on a topic.
- *Homeland Security Monitors.* These are produced monthly in collaboration with the components and may be classified or unclassified. Examples include:
  - Border Security Monitor
  - Cyber Security Monitor
  - Cuba-Gram
- *Reference Aids.* These are less analytical and more descriptive. For example, they might describe what an anthrax lab looks like or the latest on improvised explosive devices (IED) and fuses. They contain photos and diagrams and inform

[47] DHS, *Homeland Security Threat Assessment*, Executive Summary, Aug 2007, p. 1.

law enforcement and first responders what to look for and what actions to take if they are encountered.

- *Perspective.* These are longer term analytic pieces.
- *Joint Homeland Security Assessment/FBI Intelligence Bulletin.* These are joint reports done in conjunction with the FBI.

I&A also produces Homeland Intelligence Reports (HIR) which contain information that has yet to be fully evaluated. These are similar to the Intelligence Information Report (IIR)[48] produced by other IC agencies. An HIR could contain information related to border encounters, information shared by a state or local fusion center, or other information of homeland security interest. There are also Homeland Security Intelligence Reports (HSIR) that are produced by the DHS component agencies. HSIR's, however, do contain some analysis.

I&A makes the products of its analysis available to state and local officials through classified and unclassified intelligence networks:[49] The Homeland Security Information Network (HSIN) is a secured, web-based platform that facilitates Sensitive But Unclassified information sharing and collaboration between federal, state, local, tribal, private sector, and international partners. It is managed by the DHS Directorate of Operations Coordination and Planning. The HSIN platform 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.[50] It provides real-time, interactive connectivity between states and major urban areas and the National Operations Center (NOC).[51]

There are five community of interest portals on HSIN: Emergency Management, Critical Sectors, Law Enforcement, Multi-Mission Agencies, and Intelligence and Analysis (HSIN-Intelligence). The latter portal provides state, local, and tribal authorities access to unclassified intelligence products. The Homeland Security State and Local Intelligence Community of Interest (HS-SLIC) is a nationwide, virtual community of intelligence analysts that operates on a special portal on the HSIN network. The system contains collaborative tools such as discussion thread, chat tool, and secure messaging through which analysts collaborate. HS-SLIC has members from 45 states, the District of Columbia, and seven Federal agencies. The Under Secretary has established a governance board for HS-SLIC with strong participation by state and local officials.

The Homeland Secure Data Network (HSDN) provides access to collateral Secret-level terrorism-related information. This includes *NCTC Online,* a classified repository that serves as the counterterrorism community's library of terrorism information.[52] I&A has deployed HSDN

[48] An IIR is the primary vehicle used to provide human intelligence information to the consumer. It utilizes a message format structure that supports automated data entry into intelligence community databases. See JP 1-02, *DOD Dictionary of Military and Associated Terms*, Apr. 12, 2001, (as amended Oct. 17, 2008), p. 271. http://www.dtic.mil/doctrine/jel/doddict/. Hereafter: *DOD Dictionary*.

[49] Allen Testimony, Sep. 24, 2008.

[50] See DHS, *HSIN*, Feb. 10, 2009. http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm

[51] The NOC, located at the DHS Headquarters in Washington, D.C., operates on a 24/7 basis as the primary national-level hub for domestic incident management, operations coordination, and situational awareness. It is staffed by numerous Federal, state, and local agencies and fuses law enforcement, national intelligence, emergency response and private sector reporting. The NOC also has an Intelligence Watch and Warning (IWW) cell staffed with analysts from I&A. See OMB: *USG FY10 Budget*, p. 507.

[52] NCTC, *NCTC and Information Sharing*, September 2006. http://74.125.95.132/search?q=cache:7wjky-v3tA0J:www.nctc.gov/docs/report_card_final.pdf+NCTC+Online&cd=1&hl=en&ct=clnk&gl=us

terminals to 33 state and local fusion centers and intends to install terminals in all of the fusion centers as soon as security requirements are met.[53]

Intelligence Support To State, Local, Tribal Officials, and the Private Sector

A longstanding challenge for the department is the focus of I&A analysis and the relevance of its products to state, local, tribal, and private sector customers.[54] For example, at a homeland security forum in early 2008, some state and local participants expressed unhappiness with the flow of intelligence from DHS. According to the forum's findings, published in the journal *Homeland Security Affairs*, "[t]he Department had become 'irrelevant' to states and localities as a source of intelligence, because that intelligence lacks timeliness and adds so little value to local terrorism efforts. Another participant noted that 'the stream of intelligence from DHS is useless ... '"[55] Among efforts to address the issue, former Under Secretary Allen established a State and Local Fusion Center (SLFC) Pilot Project Team in 2006 to work with six fusion centers[56] in five states to enhance DHS support.

State and Local Fusion Center Program

In an effort to strengthen intelligence and information sharing and analysis capabilities following the 9/11 attacks, states and major urban areas established intelligence fusion centers.[57] Congress has defined fusion centers as a "collaborative effort of two or more Federal, state, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity."[58] At the end of 2009, there were 72 DHS/FBI designated state and Urban Area Security Initiative (UASI) fusion centers.[59]

Congress mandated that DHS support fusion centers in the Implementing Recommendations of the 9/11 Commission Act of 2007.[60] Through the DHS State, Local, and Regional Fusion Center Initiative, I&A supports these centers by providing operational, analytic, reporting, and management advice and assistance; training; information technology systems and connectivity; and intelligence officers and analysts to participating fusion centers to the maximum extent practicable.[61]

---

[53] Wagner Testimony, Mar. 4, 2010. p. 3.

[54] The Government Accountability Office (GAO) has ongoing work regarding I&A's efforts to support information sharing with state, local, and tribal government agencies. GAO expects to report on the results of this work later in 2010.

[55] Paul Stockton and Patrick S. Roberts, "Findings from the Forum on Homeland Security After the Bush Administration: Next Steps in Building Unity of Effort," *Homeland Security Affairs*, Vol. IV, No. 2,, June 2008, p.6.

[56] Pilot sites were the Boston Regional Intelligence Center and the Commonwealth Fusion Center in Massachusetts, the Florida Fusion Center, the New York State Intelligence Center, the Statewide Terrorism and Intelligence Center in Illinois, and the Regional Terrorism Threat Analysis Center in Sacramento, California.

[57] For a full discussion of fusion centers, see CRS Report RL34070, *Fusion Centers: Issues and Options for Congress*, by John Rollins. For an informative discussion of one of the earliest efforts at local law enforcement collaboration and intelligence fusion and analysis, see John Sullivan and Alain Bauer, *Los Angeles Terrorist Early Warning Group*, published by the Los Angeles County Sheriff's Department in 2008.

[58] P.L. 110-53, §511, 121 STAT. 322. Amends *Homeland Security Act of 2002* by adding §210A(j).

[59] National Criminal Intelligence Resource Center; Tallahassee, Florida; Nov. 4, 2009.

[60] P.L. 110-53, §511, 121 STAT. 318. Amends *Homeland Security Act of 2002* by adding §210A(a).

[61] Ibid. 121 STAT. 319. Amends *Homeland Security Act of 2002* by adding §210A(b) and (c).

I&A intelligence officers assigned to fusion centers are responsible for providing intelligence support, including briefings to state and local officials; reviewing and analyzing suspicious activity reports and writing HIRs based on state and local information; supporting the development of state and local intelligence products; posting material on the HSDN and the HS-SLIC portal; and reaching back to I&A for intelligence products and IT resources.

As of March 2010, there are 57 officers deployed to fusion centers and Under Secretary Wagner has stated that DHS plans to deploy a total of 76 officers (there would be more than one officer at some fusion centers) by the end of FY2010.[62] In interviews of several fusion center directors for this report, those that had I&A officers assigned to their centers were pleased with the contributions they were making. The directors who did not have an officer assigned were anxious to get one.[63]

Intelligence Threat Assessment and Coordination Group (ITACG)

Another program intended to improve the focus, relevance, and accessibility of federal intelligence products for state, local, and tribal officials is the ITACG. In 2007, Congress amended the Homeland Security Act by directing the establishment of the ITACG at NCTC to "improve information sharing within the scope of the Information Sharing Environment ...with state, local, tribal, and private sector officials."[64] Among the objectives of the ITACG is to provide a formal mechanism to inject a state, local, tribal and private sector perspective about the types of intelligence products they need and how these products should be produced and disseminated in order to be of greatest value for these officials.

The ITACG consists of two elements, an ITACG Advisory Council to set policy and develop processes for the integration, analysis and dissemination of federally-coordinated information; and an ITACG Detail comprised of state, local, and tribal homeland security and law enforcement officers and intelligence analysts detailed to work at NCTC with federal intelligence analysts.[65] The Under Secretary for I&A, as the Secretary's designee, was directed to establish and maintain the ITACG Detail and assign a senior intelligence officer from the department, who would report directly to the Director of NCTC and manage the Detail on a day-to-day basis.[66]

One historical barrier to the sharing of intelligence information with state, local, and tribal officials has been the need to protect the sources and methods used to obtain the intelligence information. The requirement for security clearances and "the need to know" principle have been cited as impediments to access by these officials. But, as one observer has pointed out, "The local deputy or officer is not interested in the sources of the information nor the means that were utilized to obtain it. The deputy or officer does need the tactic, technique, procedure, method, or resource being reported on to ensure he or she recognizes precursors of an attack when encountered on the streets."[67] The ITACG Detail is intended to educate and advise NCTC analysts about state, local, tribal, and private sector requirements, and then assist those analysts in

[62] Wagner Testimony, Mar. 4, 2010. p. 3.

[63] Comments to CRS by state and local officials, 2008.

[64] P.L. 110-53, §521, 121 STAT. 328. Amends *Homeland Security Act of 2002* by adding §210D(a).

[65] Ibid. Amends *Homeland Security Act of 2002* by adding §210D(b).

[66] Ibid, 121 STAT. 330. Amends *Homeland Security Act of 2002* by adding §210E.

[67] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *A Report Card on Homeland Security Information Sharing*, Testimony of Lee Baca, Sheriff, Los Angeles County, 110th Cong., 2nd sess., September 24, 2008, p. 3.

the preparation of versions of the products at the lowest possible level of classification to make them accessible to those customers.

As of November 2009, the Detail consists of five state and local law enforcement officers and a fire services officer. The Detail and the Advisory Council have agreed on the need for increased representation, specifically in the areas of tribal operations; homeland security planning and operations at the State and local level; health and human services; and State and local intelligence analysis. The intent is to grow the ITACG Detail to a full complement of ten SLT representatives.[68]

The ITACG Detail has been operational since late January 2008, so it may be too early to judge how effective it has been in influencing the IC's production and dissemination of intelligence products at a level of classification useful for state, local, tribal, and private sector consumers. In its November 2009 report to Congress on the ITACG, the PM-ISE reported the following achievements of the ITACG detail:[69]

- Informs and helps shape IC products for state and local agencies by reviewing, and when appropriate, providing comments during the drafting phase of the process. Since its inception, the Detail has participated in the production of 214 intelligence products.
- Created the *Roll Call Release* (RCR), a collaborative For Official Use Only (FOUO) product produced by DHS, FBI, and the Detail. The product is written specifically for state, local, and tribal (SLT) "street-level" first responders and focuses on terrorist tactics, techniques, procedures, terrorism trends, and indicators of suspicious activity. The success of this product can be measured by its incorporation into SLT-created publications and from the interest the product has also drawn from international law enforcement partners. Since the product line was created in December 2008, 26 RCRs have been published.
- Works closely with NCTC's Operations Center in the preparation of the *Terrorism Summary* (TERRSUM). The TERRSUM is a daily, SECRET- level digest of intelligence deemed to be of potential interest to SLT entities. Since its inception in June 2008, over 350 TERRSUM products have been published. Approximately 45 percent of the articles included in the TERRSUMs have been suggested by the ITACG Detail.
- The *ITACG Intelligence Guide for First Responders* was developed by SLT and federal members of the ITACG to assist SLT first responders in accessing and understanding federal intelligence reporting. The guide helps first responders understand IC jargon and acronyms, provides awareness of what information is available to them, how to access this information, and to help them understand threat reporting. The guide has been posted to several Internet websites and official unclassified portals. In addition, the guide has been mailed to over 16,000 police departments and 32,000 fire departments across the United States, Guam, Puerto Rico, and the Virgin Islands.

[68] Program Manager for the Information Sharing Environment; *Report on the ITACG, Second Report for the Congress of the United States, the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence,* Nov. 2009, pp. 6-7. http://www.ise.gov/docs/ITACG_Status_Report_PM_ISE_FINAL_24Nov09.pdf

[69] Ibid, pp. 10-11.

A senior police official at a major police department commented that "the ITACG is a good step forward, but the problem is that the IC still has a 'Cold War' mindset. The culture needs to change." He did, however, acknowledge being told by a law enforcement member of the ITACG Detail that "when he [the Detail member] reviews products and highlights things, 'the light bulbs are coming on at NCTC.' It is beginning to manifest itself in how the product is written, focusing on the right priorities."[70]

However, one senior police official is concerned that "the ITACG is limited to editing intelligence and returning those products to originating agencies where the information may or may not reach state and local law enforcement personnel."[71] This police official recommends that the ITACG "be authorized as an approved dissemination point for state and local fusion centers nationwide. ITACG liaison personnel are necessary to maintain a flow of current intelligence and must have authority to release information to state and local agencies."[72]

Mission Integration

This Office of the Deputy Under Secretary for Mission Integration (DU/S-M) is responsible for DHS IE integration activities; policies governing enterprise-wide production and standardization of reports; the I&A Strategic Plan; training, and the implementation of a comprehensive information systems architecture.[73] As part of its integration responsibilities, the DU/S-M is responsible for program review, department-level analysis, and cross-cutting intelligence initiatives. The DU/S-M also chairs the Intelligence Career Management Board that reports to the HSIC and is responsible for developing core competencies for the intelligence cadre of the Department. It does this through a document called the *Learning Road Map* that describes the tasks intelligence professionals perform, lists the training courses and other opportunities to learn the tasks, and provides measures to assess performance.[74]

The DU/S-M organization also manages I&A responsibilities for the Department's Counterintelligence (CI) Program and the Integrated Border Intelligence Program.

Integrated Border Intelligence Program (IBIP)

I&A established the IBIP to enhance its support to border security activities. Under the program, additional personnel and support infrastructure have been committed to support all of the Department's border security operations. The program is designed to link DHS intelligence resources, and those of state and local partners, with the IC in order to deliver actionable intelligence to front-line operators and to fuse national intelligence with law enforcement information.

An important initiative within the IBIP is the Homeland Intelligence Support Team (HIST). The first HIST team was deployed in 2007 to El Paso, Texas. It consists of intelligence officers from

[70] Interview with CRS, Aug. 6, 2008.

[71] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *The Future of Fusion Centers: Potential Problems and Dangers*, Testimony of Leroy D. Baca; Sheriff, Los Angeles County, 111th Cong., 1st sess., April 1, 2009, p. 3.

[72] Ibid, p. 4.

[73] A progress report on the department's efforts to establish a comprehensive information technology network architecture was submitted to Congress last year. See DHS I&A, *Homeland Security Information Technology Network Architecture Progress Report,* April 15, 2008.

[74] DHS I&A, *Learning Road Map for Intelligence Professionals – Analytics*. p. 3.

I&A whose mission is to coordinate and facilitate the delivery of national intelligence and enhance information fusion to support DHS operational missions at the border. In this regard it serves as a bridge between the national and field levels and between I&A and the component intelligence staffs at the border. It can also push/pull information from state and local law enforcement officials. The HIST also helps provide context to I&A analysts on topics such as border violence. Its focus areas are alien smuggling, border violence, weapons trafficking, illicit finance, drug trafficking, and the nexus between crime and terrorism. Its location at the El Paso Intelligence Center (EPIC)[75] gives the HIST staff immediate access to each of the DHS operational components plus 15 other Federal, state, and local agencies.

I&A has also increased staffing of the "Borders Branch" within I&A's analytic element. One senior I&A official cited this as an example of an evolving focus away from purely terrorism issues to enhanced support for specific departmental concerns. In 2005, there were only three analysts working border issues. By mid-2008, there were 20 on the border team. In the same three years, I&A increased the production of HIR's from 600, of which 3% were related to the border, to 3,563 in FY2008,[76] of which 22% were border related.[77]

National Applications Office (NAO).

For more than 30 years, the Civil Applications Committee (CAC) has facilitated requests by civil agencies to make use of space-based imaging and remote sensing capabilities in support of traditional mapping applications, as well as a broad range of resource management, environmental climate natural disaster, and remote sensing applications.[78] In its September 2005 report, a DNI study group unanimously recommended that the scope of the CAC be expanded beyond civil applications to include homeland security and law enforcement applications. In May 2007, the DNI designated DHS to be executive agent and functional manager of the NAO whose mission is to facilitate the use of IC technological assets for those purposes.[79] I&A placed this office within the DU/S-M organization.

The establishment of this office, however, has been controversial.[80] In 2008, Congress prohibited the use of funds "to commence or continue operations of the NAO until the Secretary of Homeland Security certifies in FY2009 that NAO programs comply with all existing laws,

---

[75] EPIC was established in 1974 as an intelligence center to collect and disseminate information relating to drug, alien, and weapon smuggling in support of field enforcement entities throughout the region. Following 9/11, counterterrorism also became part of its mission. In response to increased multiagency needs, EPIC has developed into a fully coordinated, tactical intelligence center supported by databases and resources from member agencies. It is jointly operated by the Drug Enforcement Administration (DEA) and CBP. Other agencies represented at EPIC include ICE; USCG; USSS; DOD, Department of the Interior; FBI; Bureau of Alcohol, Tobacco, Firearms and Explosives; U.S. Marshals Service; Federal Aviation Administration; National Drug Intelligence Center; Internal Revenue Service; National Geospatial–Intelligence Agency; Joint Task Force–North; Joint Interagency Task Force–South; Texas Department of Public Safety; Texas Air National Guard; and the El Paso County Sheriff's Office. See DEA, *El Paso Intelligence Center*. http://www.usdoj.gov/dea/programs/epic.htm

[76] DHS, *DHS Annual Performance Report, FY2008-10*, p. 99. http://www.dhs.gov/xlibrary/assets/cfo_apr_fy2008.pdf

[77] Interview with I&A senior manager, June 19, 2008.

[78] U.S. Department of the Interior, *Budget Justifications and Performance Information Fiscal Year 2011*, pp. I-17-18. http://www.doi.gov//budget/2011/data/greenbook/FY2011_USGS_Greenbook.pdf . Hereafter: DOI, *Budget Justification,* FY2011.

[79] DHS, *Fact Sheet: National Applications Office*, Aug. 15, 2007. http://www.dhs.gov/xnews/releases/pr_1187188414685.shtm

[80] For further background on the controversy surrounding the NAO, see CRS Report RL34421, *Satellite Surveillance: Domestic Issues*, by Richard A. Best Jr. and Jennifer K. Elsea.

including all applicable privacy and civil liberties standards and that clear definitions of all proposed domains are established and auditable."[81] Congress also required the Government Accountability Office (GAO) to review the certification and report to Congress.[82]

After the Obama Administration took office, DHS revisited the need for an NAO program. On June 23, 2009, after a five-month review, which the department stated was conducted in coordination with its law enforcement, emergency management, and intelligence partners, Secretary Napolitano announced her decision to end the NAO program.[83]

The CAC will continue to foster information sharing for the civil community and will seek to provide CAC members access to the skills and information necessary to protect and maximize the use of assets; facilitate relationships between the Civil and the Intelligence communities to identify and document their requirements; and expand a monthly inter-community forum for technology and information exchange to a much broader audience.[84]

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

HITRAC is the Department's infrastructure-intelligence fusion center. It is not a formal part of I&A, but is jointly resourced and managed by I&A and the Office of Infrastructure Protection, an office within the DHS National Protection and Programs Directorate. HITRAC's mission is to produce and disseminate timely and meaningful threat- and risk-informed analytic products that can effectively influence the development of infrastructure protection strategies.[85] Its use of intelligence and infrastructure expertise to support risk management decision making is illustrated at **Figure 3.**

[81] P.L. 110-329, Sep. 30, 2008, §518(a)2.c.

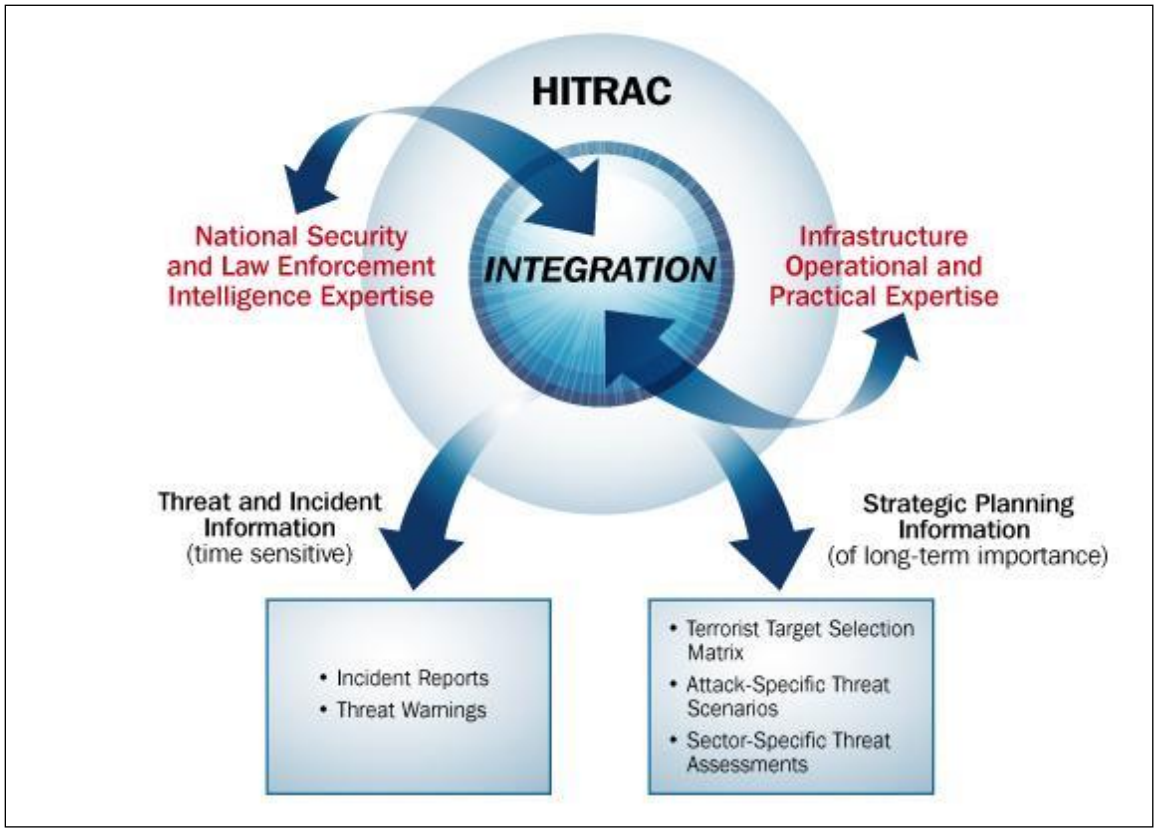
[82] An initial certification review was completed by GAO in 2008. See GAO memo to Congressional Committees, Nov. 6, 2008.

[83] DHS Press Release, "Secretary Napolitano Announces Decision to End National Applications Office," June 23, 2009. http://www.dhs.gov/ynews/releases/pr_1245785980174.shtm

[84] DOI, *Budget Justification*, FY2011, p. I-18.

[85] DHS, HITRAC Briefing for CRS on programs and services.

Figure 3. Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)



Source: DHS HITRAC, Dec. 29, 2008.

HITRAC is organized into two divisions responsible for the Center's principal functions.[86] The Risk Analysis Division performs infrastructure risk analysis and prioritization to support decision making. The division manages Congressionally-mandated and priority initiatives, including the Tier 1 and Tier 2 Program[87] and the Critical Foreign Dependencies Initiative (CFDI).[88] The Threat Analysis Division provides three services: critical infrastructure threat analysis, cyber threat analysis, and regional threat analysis including threat assessments to support the Committee on Foreign Investment in the United States (CFIUS).[89]

[86] Ibid.

[87] The Tier 1/Tier 2 Program is intended to identify the Nation's most critical, highly consequential assets and systems. The over 3,000 Tier 1/Tier2 assets and systems are those that, if disrupted, could create a combination of significant casualties, major economic loss, and/or widespread disruptions in governance and nationally critical missions. The Tier 1/Tier 2 Lists are the key components of the Urban Areas Security Initiative and State Homeland Security Grant Programs' infrastructure index, as well as other key infrastructure protection programs. See DHS, *National Critical Infrastructure Prioritization Program, Tier 1 and Tier 2 Program Overview*. http://www.nonaiswa.org/wordpress/wp-content/uploads/2009/03/national.ppt

[88] CFDI identifies important foreign infrastructure that if attacked or destroyed would critically impact the U.S. The prioritized National Critical Foreign Dependencies List (NCFDL) currently contains over 300 assets and systems in over 50 countries. See DHS, *Fact Sheet: Critical Infrastructure and Homeland Security Protection Accomplishments*, Sep. 5, 2008. http://www.dhs.gov/xnews/releases/pr_1220878057557.shtm

[89] CFIUS is an interagency committee chaired by the Secretary of the Treasury that reviews transactions that could result in control of a U.S. business by a foreign person in order to determine the effect of such transactions on the

HITRAC products[90] include State Threat Assessments that support the State Homeland Security Grant Program; Regional Infrastructure Assessments; Strategic Sector Assessment that provide an overall assessment of potential terrorist threats to critical infrastructure and key resources; Quarterly Suspicious Activity Analysis of suspicious incident reports to identify signs or patterns of activity that might pose a threat; Infrastructure Intelligence Notes that provides the private sector with a timely perspective on events, activities, or information of importance to support their specific sector-level security planning; and Homeland Security Assessments and Joint Homeland Security Assessments that communicate intelligence information that impacts the security of U.S. persons and infrastructure.

Operations Coordination and Planning Directorate (OPS)—Intelligence Division

In an effort "to improve its operations coordination and planning capability for non-routine, multi-Component operations to protect, prevent, respond to, and recover from significant threats and hazards,[91] former Secretary Chertoff in 2008 directed the enhancement of an already extant DHS organization—OPS—which was built on the foundation of the former Office of Operations Coordination. I&A provides staff to the OPS Intelligence Division, including its director.

A persistent challenge for the Department since its founding has been the integration of 22 legacy and newly-created agencies. Although the Homeland Security Act of 2002 transferred most operational responsibilities to DHS, many of these components derive their authorities from earlier legislation.[92] The execution of these authorities and responsibilities provides them with nominal operational independence. The Department has sought to develop a robust, department-wide operations planning and coordination capability to support DHS integration. But, when operational activities involve only one or two components or routine operations, the need and incentive for "department-level" planning and coordination is diminished.

A further imperative for department-wide operational planning and coordination is to support crisis and contingency planning and operations to support the Secretary of Homeland Security in his/her HSPD-5 role as the principal Federal official for domestic incident management.[93] That

national security of the United States. The DHS Directorate of Policy reviews each case and makes a recommendation to the Secretary of Homeland Security regarding the DHS position on the case. HITRAC prepares risk assessments to support the Directorate of Policy's review. See Department of the Treasury, Office of Investment Security, *CFIUS,* Feb. 20, 2009.

[90] DHS, HITRAC Information Briefing to CRS, Dec. 12, 2008.

[91] DHS, Memorandum from Secretary Chertoff to DHS Components, "Enhancement of DHS Operations Coordination and Planning Capability," May 22, 2008, p. 1. Hereafter: Chertoff Memo, May 22, 2008.

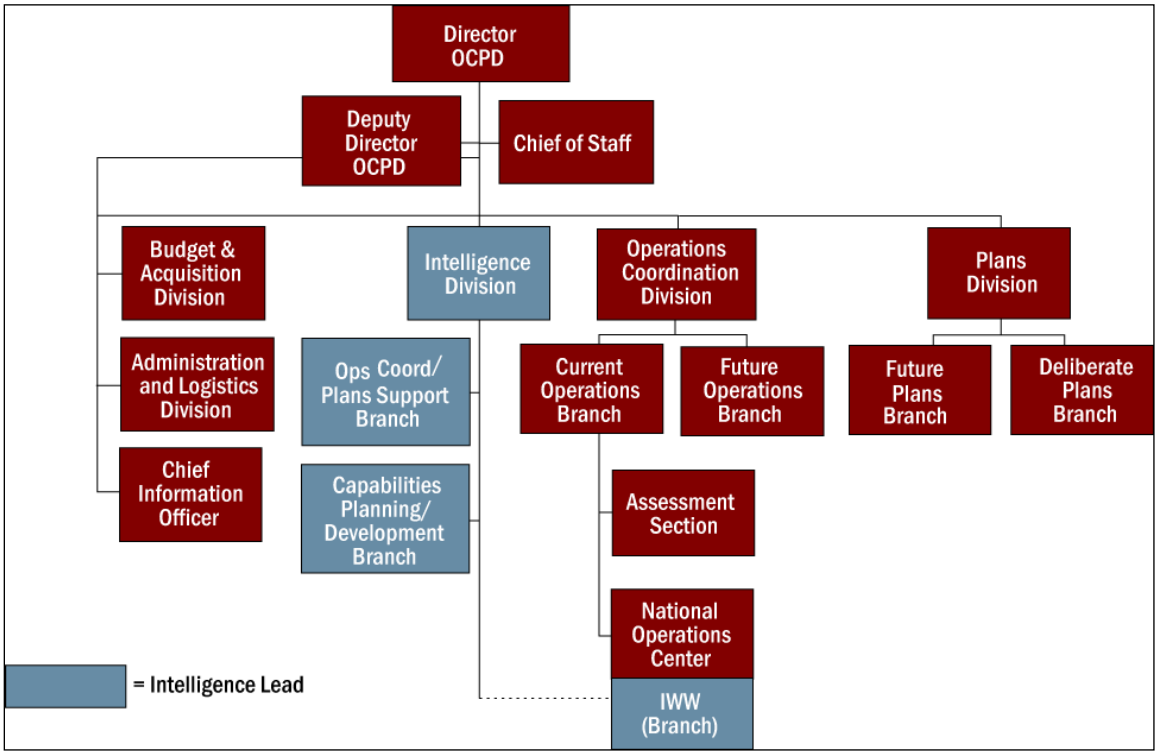
[92] For example, the statutory authority for most Federal disaster response activities especially as they pertain to the Federal Emergency Management Agency (FEMA), is the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, P.L. 100-707, Nov. 23, 1988. Authority for immigration enforcement and administration is the *Immigration and Nationalization Act of 1952* (codified as amended at 8 U.S.C. §1101); Customs authorities are generally derived from the *Tariff Act of 1930*, June 17, 1930 (see 19 U.S.C. §§1461, 1467, 1496, 1581, and 1582). Section 114(d) of the *Aviation and Transportation Security Act of 2001*, P.L. 107-71, Nov. 19, 2001, (now codified as 49 U.S.C. §114), assigned TSA responsibility for security of all modes of transportation. The USCG derives authority for its 11 mission programs from many statutes. The authority, for example, to make inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and U.S. territorial waters is 14 U.S.C. §89.

[93] According to Homeland Security Presidential Directive (HSPD)-5, *Management of Domestic Incidents*, February 28, 2003: "To prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management....The Secretary of Homeland Security is the principal Federal official for domestic incident

role not only involves coordinating activities within DHS and its components, but also all "Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies."[94]

The Intelligence Division at OPS is staffed by selected I&A personnel who provide timely, tailored intelligence products and services to support Departmental and interagency plans and operational coordination efforts. The division reaches back to, coordinates with, and leverages I&A parent elements, I&A representatives at state and local fusion centers, component intelligence organizations, and IC agencies as required, for threat-related intelligence, analysis, and other support.[95] How the division is integrated into the OPS structure is shown in **Figure 4**.

Figure 4. Directorate of Operations Coordination and Planning Organization



Source: DHS OPS, June 22, 2008.

In short, the key function of the OPS Intelligence Division is the application of intelligence research and analysis to conditions on the ground that must be considered for effective planning and operations and the development of a Common Intelligence Picture (CIP).

Former Secretary Chertoff provided insight into what a Common Intelligence Picture for DHS should look like:

> Understanding the enemy's intent and capabilities affects how we operate at our borders, how we assess risk in protecting infrastructure, how we discern the kind of threats for which we must be prepared to respond…. We need to have a common picture across this

management." http://www.fas.org/irp/offdocs/nspd/hspd-5.html

[94] HSPD-5, paragraph 4.

[95] Chertoff Memo, May 22, 2008, p. 2.

> Department, of the intelligence that we generate and the intelligence that we require. We need to fuse that information and combine it with information from other members of the intelligence community, as well as information from our state and local and international partners.[96]

Contributing to the development of a Common Intelligence Picture for the department as a whole is one of the important roles for the OPS Intelligence Division.

U.S. Customs and Border Protection (CBP) Intelligence Element

CBP is the agency responsible for securing the nation's borders at and between ports of entry (POE).[97] It was established in 2003, as a result of the Homeland Security Act of 2002, consolidating the inspection and patrol functions of the legacy U.S. Customs Service, the Immigration and Naturalization Service (INS), the U.S. Border Patrol (BP), and the Animal and Plant Health Inspection Service (APHIS).[98] CBP's primary mission is to prevent the entry of terrorists and the instruments of terrorism into the United States. But it also has responsibility to prevent illegal immigration; regulate and facilitate international trade; collect import duties; enforce U.S. trade and drug laws; and protect Americans and U.S. agricultural and economic interests by preventing the importation of harmful pests, diseases, and contaminated, diseased, infested, or adulterated agricultural and food products.

CBP accomplishes its various missions by inspecting persons and goods to determine if they are authorized to enter the United States. CBP officers and Border Patrol agents intercept illegal narcotics, firearms, counterfeit merchandise, and other types of contraband. They also interdict unauthorized aliens and enforce more than 400 laws and regulations at the border.

CBP Office of Intelligence and Operations Coordination (OIOC)

In October 2007, CBP reorganized its intelligence and anti-terrorism functions by establishing the OIOC headed by an Assistant Commissioner. It provides intelligence support to CBP's effort to detect, identify, target, and interdict terrorists, terrorist threats, weapons of mass destruction (WMD), illegal aliens and alien smuggling groups, narcotics traffickers, and other criminals attempting to penetrate or use the borders of the United States to facilitate their illegal activities.[99]

The Assistant Commissioner for OIOC is also responsible for managing the *coordination* of field operations among and beyond CBP elements and for CBP's continuity of operations program.[100] The OIOC also functions as the situational awareness hub for CBP providing timely and relevant information and actionable intelligence to operators and decision-makers. The OIOC is divided into four divisions, Incident Management, Field Coordination, Analysis and Targeting, and

[96] Chertoff, "DHS Second Stage Review Remarks."

[97] A "Port of Entry" or POE, is an officially designated location (seaports, airports, and or land border locations) where CBP officers or employees are assigned to accept entries of merchandise, clear passengers, collect duties, and enforce the various provisions of CBP and related laws. Ports also perform agriculture inspections to protect the United States from potential carriers of animal and plant pests or diseases that could cause serious damage to America's crops, livestock, pets, and the environment. See CBP, "Ports of Entry and User Fee Airports." http://www.cbp.gov/xp/cgov/trade/trade_outreach/ports.xml.

[98] P.L. 107-296, Subtitles C and D.

[99] CBP, "OIOC Organizational Information." http://www.cbp.gov/xp/cgov/about/organization/assist_comm_off/

[100] Ibid.

Intelligence and Situational Awareness. OIOC analysts are stationed at its headquarters and are posted to other agencies in a liaison capacity, such as NCTC, the NJTTF, and the Human Smuggling and Trafficking Center (HSTC).

CBP Intelligence Support to DHS and CBP Missions.

CBP intelligence operations are designed to support the full range of CBP missions, particularly its primary mission of preventing the entry of terrorists and the instruments of terrorism. To that end, the CBP OIOC is engaged in the entire intelligence cycle, including planning, collection, processing, production, and dissemination of "all source" information and intelligence to support CBP's operational elements, as well as their partners within DHS and other government agencies.[101]

Although CBP does not engage in traditional foreign intelligence collection activities, it receives information from DHS I&A, the IC, and law enforcement agencies. In addition, CBP gathers and analyzes large amounts of data concerning persons and cargo inbound to the U.S. as well as information derived from the apprehensions of illegal aliens, drug seizures, and other border enforcement activities. For example, CBP collects advance passenger information (API)[102] for all air and ship passengers and crew traveling to or from the United States. During its border inspection activities, CBP officers may also examine documents, books, and other printed material, as well as computers disks, hard drives, and other electronic or digital storage devices.[103] All of this data is a unique source of operational intelligence that is potentially very useful to other Federal agencies with national security missions. The border environments in which the CBP offices operate illustrate how intelligence supports DHS and CBP mission activities.

At Ports of Entry

CBP officers conduct screening activities to determine the admissibility of persons and goods and interdict dangerous people, dangerous items, and contraband. Given the volume of people and goods seeking entry into the U.S. every year, it is impractical for CBP to physically inspect every person or shipment that arrives at a U.S. port.[104] Therefore, CBP analyzes trade data and cargo, crew, and passenger manifest information to 'target' its inspection resources towards those persons or cargo shipments that potentially pose the highest risk. Intelligence from other Federal

[101] CBP, "Commissioner's Message – New Office of Intelligence and Operations Coordination," July 23, 2007.

[102] API data consists of the information on the biographical page of the person's passport, plus additional information on the flight or voyage generated by the airline or shipping line. API includes the traveler's surname, first name, and any middle names; date of birth; gender; citizenship; and type of travel document used for identification, document number, and place of issue. API also includes departure point and time, arrival point and time, and air carrier and flight number.

[103] A CBP officer's border search authority is derived from federal statutes and regulations, including 19 C.F.R. 162.6, which states that, "All persons, baggage and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection by a CBP officer." Unless exempt by diplomatic status, all persons entering the United States, including U.S. citizens, are subject to examination and search by CBP officers. Source: CBP, "CBP Authority to Search," June 12, 2008. Hereafter: "CBP Authority to Search." http://www.cbp.gov/xp/cgov/travel/admissibility/authority_to_search.xml

[104] In FY2009, at 327 ports of entry, CBP inspected over 361 million travelers; 109 million cars, trucks, buses, trains, vessels, and aircraft; encountered 224,000 inadmissible aliens; seized more than 1.5 million pounds of illegal narcotics; and seized over 1.5 million prohibited meat, plant materials or animal products, including 166,727 agricultural pests. Source: CBP, *Securing America's Borders – CBP 2009 Fiscal Year in Review*, November 24, 2009. http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2009_news_releases/nov_09/11242009_5.xml

agencies, in the form of 'lookouts,' and other law enforcement and intelligence reporting, is also reviewed.

The targeting mechanism used by CBP is the Automated Targeting System (ATS). ATS is composed of six modules that focus on exports, imports, passengers and crew (airline passenger and crew on international flights, passengers and crew on sea carriers), private vehicles crossing at land borders, and import trends over time. These modules employ weighted rule sets[105] to identify high-risk passengers and cargo shipments.

In the cargo environment, ATS employs these rule sets to assign scores based on factors associated with risk. Above a certain threshold risk score, cargo is subject to further inspection.[106] A variety of data[107] is used within ATS to perform risk analysis. For cargo, ATS uses data from the Automated Commercial System (ACS), Automated Broker Interface (ABI), Automated Manifest System (AMS), and the new Automated Commercial Environment.[108]

The passenger component of ATS (ATS-P) processes traveler information against other information available to ATS, and applies threat-based scenarios comprised of risk-based rules to assist CBP officers in identifying individuals who require additional screening or in determining whether individuals should be allowed or denied entry into the United States. The risk-based rules are derived from discrete data elements, including criteria that pertain to specific operational/tactical objectives or local enforcement efforts.

Unlike in the cargo environment, ATS-P does not use a score to determine an individual's risk level. Instead, it compares Passenger Name Record (PNR) [109] and information in the following databases against lookouts and patterns of suspicious activity identified by analysts based upon past investigations and intelligence.

- Treasury Enforcement Communications System (TECS)[110]

---

[105] These rules are developed using sophisticated concepts of business activity intended to identify suspicious or unusual behavior. See DHS Chief Privacy Officer, *Privacy Impact Assessment (PIA) CBP ATS,* November 22, 2006, p. 3. Hereafter: *DHS Privacy Impact Assessment on ATS.*

[106] National targeting thresholds are set by the National Targeting Center and are evaluated and adjusted in response to intelligence and analysis.

[107] Data include electronically filed bills, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land border crossing and referral records for vehicles crossing the border, airline reservation data; non-immigrant entry records; and records from secondary referrals, incident logs, suspect and violator indices, and seizures. A full list of data by module can be found at *DHS Privacy Impact Assessment on ATS,* Appendix A, pp. 25-27.

[108] ACS is the legacy system used by CBP to track, control, and process all commercial goods imported into the United States. ABI is the part of ACS that permits qualified participants to file import data electronically. AMS is used by carriers to file advance declarations of their international containers and cargo contents. ACE is CBP's new import and export cargo manifest processing system intended to facilitate trade and strengthen border security. Deployed in phases, ACE will be expanded to provide cargo processing capabilities across all modes of transportation and replace existing systems with a single, multi-modal manifest system for land, air, rail and sea cargo in a secure, paper-free, web-enabled environment. See CBP, "ACE At a Glance Fact Sheet," Oct. 7, 2009. http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/ace_factsheets/ace_glance_sheet.xml

[109] PNR is the information contained within the computerized reservation systems of air and sea carriers. PNR data include, but are not limited to full itinerary; co-travelers; contact information; travel agency, form of payment; seat assignment; bag tag numbers, and changes to the reservation. A full list of PNR data fields is at *DHS Privacy Impact Assessment on ATS,* Appendix B, p. 28.

[110] TECS is a computerized information system designed to identify individuals and businesses suspected of, or involved in violation of Federal law. Resident on TECS at the CBP Data Center is the Interagency Border Information System (IBIS) which tracks information on suspected individuals, businesses, vehicles, aircraft, and vessels and includes terrorist and other law enforcement lookouts, and visa, immigration, and border crossing data. TECS also

- Advance Passenger Information System (APIS)[111]
- Non Immigrant Information System (NIIS)[112]
- Suspect and Violator Indices (SAVI)[113]
- Department of State visa databases[114]
- Passenger Name Record (PNR) systems

This risk assessment is an analysis of the threat-based scenario(s) that a traveler matched when traveling on a given flight. These scenarios are drawn from previous and current law enforcement and intelligence information. This analysis is done in advance of a traveler's arrival to or departure from the United States and becomes one tool available to DHS officers in identifying illegal activity.[115]

It was through application of the ATS-P that CBP officers at the National Targeting Center selected Umar Farouk Abdulmutallab, who attempted to detonate an explosive device on board Northwest Flight 253 on December 25, 2009, for further questioning upon his arrival at the Detroit Metropolitan Wayne County Airport POE.[116]

National Targeting Center (NTC)

The operational organization that utilizes the ATS to support CBP officers at POE's is the NTC. It is not an intelligence organization, it is part of the CBP Office of Field Operations. But it is a significant consumer of intelligence information, upon which it conducts analysis and bases recommendations for security actions. It is also a major source of information about passenger and cargo movements that can be exploited for intelligence purposes.

The NTC grew out of efforts by the legacy U.S. Customs Service to develop targeting techniques at the port level to detect drug smuggling and currency violations in both the passenger and cargo environments. Post-9/11, Customs began adapting these targeting practices towards anti-terrorist and other national security concerns. In November of 2001, following the 9/11 attacks, the NTC

---

provides access to the FBI's National Crime Information Center (NCIC) and the National Law Enforcement Telecommunication Systems (NLETS), the latter of which provides direct access to state motor vehicle departments. See "CBP Authority to Search;" and Department of Treasury, "System of Records Notice," 66 *Federal Register* 53029, Oct. 18, 2001.

[111] APIS is the electronic data interchange system for air carrier transmission to CBP of electronic passenger, crew member, and non-crew member manifest data. See DHS, "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels; Final Rule," 72 *Federal Register* 48320, Aug. 23, 2007. Hereafter referred to as *DHS Advance Electronic Transmission of Manifests Final Rule*, Aug. 23, 2007.

[112] The NIIS is a repository of records tracking persons arriving in or departing from the United States as non-immigrant visitors. See USCIS, *System Notice for Non Immigrant Information System*. http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=f63fd0676988d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=34139c7755cb9010VgnVCM10000045f3d6a1RCRD&survey=1

[113] SAVI consists of records of individuals suspected of or who have violated Customs laws. See Department of Treasury, "System of Records Notice," 66 *Federal Register* 53025 and 53031, Oct. 18, 2001.

[114] These include the Consular Lookout and Support System (CLASS), used by State Department to house information about people who have violated the terms of their visas; and the Consolidated Consular Database (CCD), which integrates State Department information used by foreign visa officers.

[115] DHS *System of Records Notice for the ATS,* p. 6.

[116] Sebastian Rotella, "U.S. Learned Intelligence on Airline Attack Suspect While He Was Enroute." Los Angeles Times.com, Jan. 7, 2010. http://articles.latimes.com/2010/jan/07/nation/la-na-airline-terror7-2010jan07

began operations on a 24/7 basis. In March 2007, the NTC was divided into two elements, NTC–Passenger and NTC–Cargo.

NTC—Passenger (NTCP)

The NTCP works closely with the OIOC and other intelligence and law enforcement organizations to develop targeting rule sets for ATS-P. They then work with analytical units located at POE's to provide targeting information and real-time response to requests from CBP officers in the field for information on potentially high-risk passengers seeking entry into the United States.[117] One of the most important sources of information analyzed by NTCP is API data which commercial carriers are required to submit to CBP on all air and ship passengers and crew traveling to the United States.[118] The data is examined to determine possible matches with various inspection systems and watchlists that include lookouts on known and suspected terrorists or other persons of interest to U.S. law enforcement agencies.

NTC—Cargo (NTCC)

The NTCC supports efforts to detect and prevent dangerous cargo from entering the United States. It examines advance electronic manifest information that CBP requires to be submitted for all modes of transportation.[119] It then uses advanced, computerized risk-assessment techniques within ATS to sort the information according to more than 100 variables. Citing security concerns, federal officials refused to list those variables, but some officials said that the port of origin, the nature of the cargo, and the track records of the exporter and importer were among the criteria.[120] In addition, the NTCC provides significant support to Cargo Security Initiative ports where CBP has stationed targeting teams to identity containers for inspection prior to their being loaded on U.S.-bound vessels.

The NTCC works closely with OIOC to develop targeting rule sets for the cargo component of ATS. They also collaborate with NTCP who notifies NTCC of any passenger matches to terrorist-related or other law enforcement lookouts. NTCC will then run those matches against various databases to determine if those individuals are involved with any cargo businesses or specific cargo shipments.

The NTCC focuses particular attention on types of cargo that could be ingredients for weapons of mass destruction (WMD), weapons of mass effect, chemical precursors of illegal drugs, and conventional weapons and explosives. Sweeps based on specified targeting parameters are conducted daily to target suspect chemical, biological, radiological, conventional weapons, explosives, and ammonium nitrate shipments.[121] In early 2008, working with ICE and DEA, this targeting identified suspicious bills of lading, which led to the seizure of chemicals associated with the manufacture of methamphetamines.[122] In late 2007, targeting and analysis within NTCC

[117] CBP, *Performance and Accountability Report, FY2007*, Nov. 13, 2007, p. 17.

[118] Effective Feb. 18, 2008, carriers must provide CBP with API data in advance of passenger boarding of aircraft or vessels. See *DHS Advance Electronic Transmission of Manifests Final Rule*, Aug. 23, 2007.

[119] Twenty-four hours in advance of lading for cargo loaded on US-bound vessels; four hours or wheels-up for international air cargo; four hours in advance of arrival for inbound rail cargo; and one hour in advance of arrival for cargo on inbound trucks (30 minutes in advance of arrival for FAST shipments).

[120] Seth Schiesel, "Their Mission: Intercepting Deadly Cargo," *New York Times*, Mar. 20, 2003.

[121] CBP, "NTCC," a briefing provided to CRS on July 21, 2008.

[122] Ibid.

led to the intercept and seizure of over $3 million worth of assault rifles and small arms destined for Central America.[123]

Between POE's

While CBP officers work primarily at POE's, Border Patrol agents patrol vast areas along the northern and southern international land borders of the United States that lie in between the POE's, as well as the coasts of Florida, Puerto Rico, and the U.S. Virgin Islands. The Office of Air and Marine (A&M) supports this mission through its operations within the air and maritime environments. Two centers that provide intelligence support to these operations are the Border Field Intelligence Center (BORFIC) and the Air and Marine Operations Center (AMOC). In addition, the Border Patrol has placed intelligence units within each of its 20 Border Patrol Sectors.[124]

OIOC supports BP and A&M with real-time intelligence and strategic analyses about the conveyances, routes, and other methods that undocumented aliens, human smugglers, drug traffickers, and other criminals use to enter or smuggle persons or contraband into the United States. An example of this strategic intelligence analysis was an April 2006 report[125] co-produced by CBP and the NCTC. The report, which surveyed the arrest records of "special interest aliens" (SIA)[126] caught at the U.S. southern border, revealed how these individuals entered the U.S. and how terrorists could exploit such vulnerabilities.

In response to this information, DHS developed and implemented a multi-pronged plan to address those vulnerabilities. The plan included targeted training and other efforts to eliminate the proliferation and use of false passports from one African country; and training to build the detection capabilities of several Western Hemisphere countries that were noted to be used by SIA's with false or altered passports in transit to the United States.

Border Field Intelligence Center (BORFIC)

Originally established as the Border *Patrol* Field Intelligence Center in 2004 in El Paso, Texas, BORFIC conducts all-source intelligence activities to support the border security mission of the BP and other DHS and CBP elements to predict, detect, deter, and interdict terrorists, terrorist weapons, and human traffickers and contraband smugglers entering the United States.[127] In October 2007, the organization was fully integrated into the CBP OIOC and its name changed to the Border Field Intelligence Center.

---

[123] Ibid.

[124] The Border Patrol Sectors (listed alphabetically): Blaine, Washington; Buffalo, New York; Del Rio, Texas; Detroit (Selfridge Air National Guard Base), Michigan; El Centro, California; El Paso, Texas; Grand Forks, North Dakota; Havre, Montana; Houlton, Maine; Laredo, Texas; Marfa, Texas; Miami, Florida; New Orleans, Louisiana; Ramey, (Aguadilla), Puerto Rico; Rio Grande Valley, Texas; San Diego, California; Spokane, Washington; Swanton, Vermont; Tucson, Arizona; and Yuma, Arizona.

[125] NCTC, *SIA Trends Reveal Vulnerabilities Along Route to U.S.,* Apr. 6, 2006.

[126] The term Special Interest Alien (SIA) covers individuals traveling illegally to the United States and originating in Afghanistan, Algeria, Bahrain, Bangladesh, Djibouti, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kazakhstan, Kuwait, Lebanon, Libya, Malaysia, Mauritania, Morocco, Oman, Pakistan, Philippines, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tajikistan, Thailand, Tunisia, Turkey, Turkmenistan, United Arab Emirates, Uzbekistan, Yemen, Gaza, and the West Bank. See Ibid., p. 1. Countries and territories are presumed to be included on the SIA list due to the connections of some of their citizens to international terrorism.

[127] CBP BORFIC, Briefing for CRS, Dec. 3, 2008.

BORFIC is responsible for supporting security efforts on both the northern and southern borders. It exchanges intelligence and law enforcement information with numerous Federal, state, local, and tribal organizations agencies and actively participates in several interagency and bilateral groups. These include the El Paso Interagency Intelligence Working Group which includes EPIC, DOD's Joint Task Force-North, and the FBI; the Bilateral Interdiction Working Group with Mexico, the Integrated Border Intelligence Teams (IBETS)[128] with Canada, and the Caribbean Border Interagency Group. BORFIC shares law enforcement intelligence information with state and local fusion centers through the HS-SLIC portal. In addition, BORFIC has four personnel assigned to the El Paso Intelligence Center (EPIC) who work in tandem with I&A's Homeland Intelligence Support Team also located there.

Air and Marine Operations Center (AMOC)

Located in Riverside, California, the AMOC is a 24/7, multi-agency coordination center that detects, sorts, and monitors air and marine tracks of interest[129] across the nation's borders and maritime approaches. A subordinate center located in Puerto Rico performs the same mission for the Caribbean region. The AMOC also serves as host activity for the central operations of CBP's long-range unmanned aircraft systems and is the CBP focal point for the coordination of unmanned aircraft system maritime operations with the USCG. The AMOC is staffed with intelligence operations specialists who provide connectivity to the OIOC, DHS, and the IC. It also has liaison officers assigned from the USCG, FAA, DOD National Guard Bureau, and the Government of Mexico.[130]

The AMOC produces a comprehensive air surveillance radar picture through its Air and Marine Operations Surveillance System (AMOSS). Fusing input from up to 450 sensors, including an extensive network of military and civilian radars across the United States and Canada, the AMOSS can process up to 24,000 fused tracks every 12 seconds and input up to 1,000 flight plans per minute.[131] This allows the AMOC to provide real-time data on suspicious or non-cooperative aircraft and marine vessels to A&M, BP, and the USCG to support interdiction operations as well as to other DHS intelligence and operations centers. In addition to aircraft and vessel location data, Detection Systems Specialists at the AMOC have access to numerous law enforcement and other databases that allow them to provide operational units with information regarding the flight plans, history, ownership, and registration of aircraft and vessels and criminal background information on pilots and vessel crew.

In addition to its land and maritime border security mission, the AMOC also supports the multi-agency effort to provide airspace security for the National Capital Region. As a participating agency within the National Capital Region Coordination Center, the AMOC provides its

[128] The IBETS are a joint effort of U.S. and Canadian law enforcement and security agencies to combine and coordinate their intelligence and law enforcement expertise to identify and stop the high-risk movement of people and goods between the ports of entry on the Canada - United States border. On the Canadian side, IBETS are co-managed by the Canadian Border Security Agency (CBSA) and the Royal Canadian Mounted Police. U.S. participating agencies are CBP, ICE, and the USCG. There are IBETs operating in 15 regions along the border. Source: CBSA, *Canada-U.S. IBETS*. http://www.cbsa-asfc.gc.ca/security-securite/ibet-eipf-eng.html#mission

[129] Among the reasons for an aircraft or vessel to be considered a track of interest is that it is unidentified, uncooperative (i.e., not responding to air traffic control or law enforcement direction), or otherwise behaving suspiciously.

[130] U.S. Government Accountability Office, *Opportunities Exist to Enhance Collaboration at 24/7 Operations Centers Staffed by Multiple DHS Agencies, 07-89,* Oct. 2006, pp. 13-14.

[131] Spanky Kirsch, "Multifunction Phased Array Radar's Contribution to Secure Skies and Borders," DHS Science and Technology Directorate, slide presentation, Oct. 11, 2007, slide 24.

comprehensive radar picture and law enforcement sorting, detection, and investigative capabilities to assist in identifying and determining the threat posed by aircraft that are not compliant with the flight rules in effect for the Washington, D.C. Metropolitan Area Air Defense Identification Zone (DC ADIZ).[132]

Intelligence Driven Special Operations (IDSO)

OIOC collaborates with CBP Office of Field Operations to develop IDSO's based on threat information. IDSO's not only address immediate threat concerns, but also serve to counter predictability in CBP inspection operations. They are enforcement actions that are based upon specific intelligence or current trends and are vetted through the DHS CINT.[133] For example, if an increase in aliens entering the United States illegally from or through a particular country were documented, CBP could develop an IDSO to intensify inspection activity on persons and routes from that country.

An IDSO based on specific intelligence was conducted following the March 2004 Madrid train bombings. CBP analysis revealed an increase in aliens attempting to enter the U.S. illegally using freight and passenger railcars along the northern border. In response, CBP assigned officers and resources to targeted POE's to intensify inspections of railcars; NTC intensified its screening of persons and cargo, the BP assisted in capturing and detaining illegal aliens; and CBP intelligence intensified its checks of foreign nationals through the IC.[134]

Immigration and Customs Enforcement (ICE) Intelligence Element

ICE is the largest investigative organization within DHS. It was established in 2003 and incorporated into DHS by consolidating the investigative elements of the former U.S. Customs Service and Immigration and Naturalization Service (INS) and by transferring the Federal Protective Service from the General Services Administration (GSA).

ICE's mission is to enforce trade and immigration laws through the investigation of activities, persons and events that may pose a threat to the safety or security of the United States and its people. OI also investigates illegal trafficking in weapons (including weapons of mass destruction), the smuggling of narcotics and other contraband, human smuggling and trafficking, money laundering and other financial crimes, fraudulent trade practices, identity and benefit fraud, child pornography, child sex tourism, and health and public safety dangers.[135] It has four operational divisions:

[132] The DC ADIZ is that area of airspace in which the ready identification, location, and control of aircraft is required in the interests of national security. Specifically, it is that airspace from the surface to 18,000 feet within a 30-mile radius of the Reagan Washington National Airport (DCA). See Federal Aviation Administration (FAA) Notice to Airmen (NOTAM) 7/0206, effective Aug. 30, 2007.

[133] Written Testimony of CBP Director of the Office of Intelligence, L. Thomas Bortmes, in U.S. Congress, Hearing of the Intelligence, Information Sharing, and Risk Assessment Subcommittee of the House Committee on Homeland Security, "DHS Intelligence and Border Security: Delivering Operational Intelligence." 109th Cong., 2nd sess., June 28, 2006, (Washington: U.S. GPO, 2007).

[134] CBP briefing to CRS, May 25, 2004.

[135] ICE, *FY2010 Enacted Budget Fact Sheet*, Nov. 5, 2009, http://www.ice.gov/pi/news/factsheets/

- Office of Investigations (OI). OI is responsible for investigating a range of issues that may threaten national security. OI uses its legal authority to investigate issues such as immigration crime, human rights violations, and human smuggling; narcotics, weapons and other types of smuggling; and financial crimes, cybercrime, and export enforcement issues.[136] Of note, ICE Special Agents are the largest non-FBI component of the Joint Terrorism Task Forces (JTTF).[137]
- Detention and Removal Operations (DRO). DRO is the primary enforcement arm within ICE for the identification, apprehension and removal of illegal aliens from the United States.[138]
- Office of International Affairs (OIA). With 63 offices in 44 countries, OIA develops partnerships with foreign governments to advance the homeland security mission.[139]
- Office of Intelligence, discussed below.

Office of Intelligence

ICE's intelligence activities are coordinated and managed within the Office of Intelligence. The office is responsible for collecting, analyzing, and disseminating strategic and tactical intelligence for use by the operational elements of ICE and DHS. ICE intelligence activities focus on information related to the movement of people, money and materials into, within and out of the United States. Its objective is to provide timely, accurate, and useful intelligence to support a range of investigative activities by identifying patterns, trends, routes, and methods of criminal activity; predicting emerging and future threats; and identifying potential systemic vulnerabilities and methods to mitigate those vulnerabilities.[140]

Although ICE is not a member of the IC, the Office of Intelligence participates in all aspects of the intelligence cycle. In support of the agency's mission, the office collects and analyzes information from a variety of sources including the IC, other federal agencies, other components of DHS, state, local, tribal, and foreign agencies. It also analyzes the considerable information derived from ICE operational activity, such as investigations, document exploitation, and interviews of detainees. Information sources include classified intelligence reporting, law enforcement sensitive information, and open source material such as commercial and trade data. Consumers of ICE intelligence products are ICE investigators; DRO and FPS officials; the ICE and DHS leadership; DHS partners, particularly CBP; the Department of State; FBI; the Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, and Firearms, and state and local law enforcement agencies.

[136] ICE, *ICE Programs, Office of Investigations*. http://www.ice.gov/investigations/index.htm

[137] Joint Terrorism Task Forces (JTTFs) are investigative units consisting of law enforcement and other specialists from dozens of U.S. Federal, state, and local law enforcement and intelligence agencies. They are led by DOJ and the FBI. The National JTTF was established in July 2002. Forty agencies are represented in the NJTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple agencies. See DOJ, *Joint Terrorism Task Force*. http://www.usdoj.gov/jttf/

[138] ICE, *ICE Programs, Detention and Removal Operations*. http://www.ice.gov/pi/dro/index.htm

[139] ICE, *About the ICE Office of International Affairs.* http://www.ice.gov/international-affairs/presence.htm

[140] ICE Office of Intelligence, *Mission Overview and Guide to Products and Services,* June 2008, p. 1.

The Office of Intelligence is led by a Director and consists of six divisions and 26 Field Intelligence Groups.[141] The Intelligence Operations Division coordinates and provides intelligence support to ICE field components, including the ICE Special Agent-in-Charge (SAC) offices, DRO field offices, and FPS regions. The Intelligence Programs Division analyzes information obtained from intelligence, law enforcement, and open sources and produces finished intelligence products to support ICE, DHS, and other intelligence and law enforcement consumers.

Intelligence Programs Division

The Intelligence Programs Division has the following specialized units: Counter Proliferation Intelligence, Human Smuggling and Public Safety (HSPSU), Contraband, Illicit Finance/Trade Fraud, and International Intelligence, and the Tactical Intelligence Center located in Bay Saint Louis, Mississippi, which works with the National Security Agency and other intelligence units to integrate and analyze signals intelligence, human intelligence, and law enforcement information to identify new criminal organization targets for ICE investigations, assist NSA in SIGINT targeting, and support other Office of Intelligence units in performing strategic level intelligence analysis.

The International and Border Support unit focuses production on two primary areas. The first is support rendered to the ICE Attachés of the Office of International Affairs through the International Intelligence Unit. The second is through another cell that provides support to Southwest Border operations that target criminal organizations operating in that region, especially those that contribute to escalating violence along the border. Southwest Border is focused on four operations: the Border Violence Intelligence Cell, Support the Border Enforcement Security Taskforces, Operation Armas Cruzdas, and Operation Firewall.

Border Violence Intelligence Cell (BVIC)

The BVIC was established in January 2008 in order to provide intelligence support for ICE weapons smuggling investigations and government-wide efforts to combat violence along the United States-Mexico border.[142] It is located at EPIC within the Crime-Terror Nexus Unit. The BVIC works closely with I&A's Homeland Intelligence Support Team, and other partners at EPIC.

As the level of violence along the U.S.- Mexican border intensified in the past two years, ICE has partnered with Mexican and other U.S. law enforcement agencies on three initiatives described below to enhance border security, disrupt transnational criminal organizations, and stop the illegal flow of firearms from the United States into Mexico. These are the Border Enforcement Security Task Forces (BEST), Armas Cruzadas, and Operation Firewall. The BVIC supports all three programs. At the BVIC, all-source intelligence is analyzed and operational leads are provided to the BEST task forces and ICE attaché offices. The BVIC also analyzes data from arrests and seizures by the BEST task forces and exchange intelligence with Mexican law enforcement agencies.

In November 2008, the BVIC, in collaboration with CBP and DHS I&A, produced an Intelligence Report, *United States Southbound Weapons Smuggling Assessment*, which examined U.S. southbound weapon smuggling trends. This report was designed to support the BEST's and other operational components in planning and conducting outbound firearms smuggling operations. In

[141] The missions of these divisions are described in detail in Ibid, pp. 2-5.

[142] ICE, *BVIC Fact Sheet*, June 2008.

December 2008, the BVIC also co-authored a strategic-level analysis for the ICE and DHS leadership on the same issue.

Border Enforcement Security Task Forces (BEST)

The BEST initiative[143] consists of a series of multi-agency investigative task forces, of which ICE is the lead agency. They seek to identify, disrupt, and dismantle criminal organizations posing significant threats to border security. Other agency participants include CBP, the Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, and Firearms (ATF), FBI, USCG, and the U.S. Attorney's offices, and state and local law enforcement. The Mexican law enforcement agency Secretaria de Seguridad Publica is a partner along the southern border. The Royal Canadian Mounted Police and Canadian Border Services Agency are partners on the northern border.

There are currently BEST task forces on both the northern and southwestern borders with ten on the southwest border. Each BEST concentrates on the prevalent threat in their area. On the southern border, this entails cross-border violence; weapons smuggling and trafficking; illegal drug and other contraband smuggling; money laundering and bulk cash smuggling; and human smuggling and trafficking. The Office of Intelligence maintains 28 analysts within the Southwest Border BESTs to ensure responsive intelligence support and appropriate information sharing with other federal, Government of Mexico, state, tribal and local law enforcement partners.[144]

Armas Cruzadas

Armas Cruzadas is a partnership between U.S. and Mexican law enforcement agencies. [145] Its objective is to synchronize bilateral law enforcement and intelligence sharing operations in order to identify, disrupt, and dismantle trans-border weapons smuggling networks. Among the activities under Armas Cruzadas, ICE Border Liaisons are deployed to the border to strengthen bilateral communication. There is also a Weapons Virtual Task Force, a virtual online community where U.S. and Mexican investigators can share intelligence and communicate in a secure environment.[146]

For the United States, ICE is a major participant agency in Armas Cruzadas because of its authority as the Federal agency responsible for investigating cases involving weapons being smuggled out of the United States. ATF participates as a result of its authority over weapons being illegally sold and transported within the United States. CBP is also a participating agency due to its border security responsibilities.

Operation Firewall

Operation Firewall is an initiative to combat bulk cash smuggling, one of the methods that transnational criminal organizations use to move the proceeds from their criminal activities to fund future operations. ICE has found that as successful enforcement has made the transfer of

[143] ICE, *BEST Fact Sheet*, Dec. 3, 2008.

[144] ICE Briefing for CRS, Jan. 21, 2010.

[145] ICE, *Armas Cruzadas Fact Sheet*, Nov. 12, 2008.

[146] U.S. Congress, Senate Committee on Judiciary, Subcommittee on Crime and Drugs, *Law Enforcement Responses to Mexican Drug Cartels*, Statement of Kumar C. Kibble, Deputy Director, ICE Office of Investigations, 111th Cong., Mar. 17, 2009.

illicit funds between banks and other financial institutions more difficult, criminal organizations are increasing their use of bulk cash smuggling.[147] Operation Firewall is a joint effort with CBP to target the full array of methods used to smuggle bulk cash, including commercial and private passenger vehicles, commercial airline shipments and passengers, and pedestrians crossing U.S. borders with Mexico and Canada. [148]

Collection Management and Requirements Division

The Collection Management and Requirements Division coordinates the intelligence collection and reports efforts within ICE. In this regard, it works closely with other DHS and IC elements to articulate ICE intelligence requirements to collection elements within the IC to ensure the flow of needed information to ICE. This division also manages the ICE Joint Intelligence Operations Center.

The Office of Intelligence also has two divisions which provide support activities, the Business Management Division and the Executive Information and Technology Division. Business Management provides support to daily operations throughout the homeland and overseas through executing procurement, budget, logistics, and training functions.

The Executive Information and Technology Division provides information technology services that support day to day operations, processing large quantities of information, and managing secure communications systems networks. This division also includes the Intelligence Document Exploitation (IDocX). Under this program, captured media, such as hard copy documents, audio recordings, and electronic media are exploited in order to develop intelligence products. Hard copy documents, for example, are converted into digitized data allowing ICE to create a vital resource for analysis, pattern recognition, and information sharing accessible to intelligence analysts and investigators.

Field Intelligence Groups (FIG)

The Office of Intelligence field organization consists of 26 FIGs that are aligned and co-located with ICE SAC offices throughout the United States. They replaced the former Field Intelligence Units in a reorganization of the ICE field intelligence structure intended to improve connectivity and working relationships with ICE operational elements and enhance coordination with other Federal, state, local, and cross border partners. [149]

Each FIG is managed by a Field Intelligence Director or advisor and is staffed by a mix of intelligence and operational personnel. FIG personnel identify and analyze criminal trends, threats, methods and systemic vulnerabilities related to ICE strategic priorities within their office's area of responsibility. FIG intelligence reports, assessments, and other products primarily support the ICE leadership and field managers, but are also disseminated to other DHS, law enforcement, and IC member agencies.

[147] U.S. Congress, House Appropriations Committee, Subcommittee on Homeland Security, *Border Security Enforcement Task Force,* Statement of Marcy Forman, Director, ICE Office of Investigations, 111th Cong., Mar. 10, 2009.

[148] ICE, *Operation Firewall Fact Sheet*, Feb 6, 2008.

[149] This summary of FIG mission and functions is from Ibid., p. 1.

Human Smuggling and Trafficking Center (HSTC)

The HSTC was established in 2004 and serves as the U.S. Government's intelligence fusion center and information clearinghouse for all federal agencies addressing human smuggling, human trafficking, and the facilitation of terrorist mobility. Human smugglers seek to profit from the illegal *transportation* of persons into a country. Human traffickers seek to profit from transporting a person into a country for the purpose of *exploiting* them. As a profitable destination for smuggled and trafficked persons, both are major problems for the United States. Numerous transnational organized crime groups are involved in the trade.

Congress formally established the HSTC in the Intelligence Reform Act and Terrorism Prevention Act of 2004. [150] In 2007, Congress strengthened the Center's manning and funding in Section 721 of the Implementing Recommendations of the 9/11 Commission Act of 2007.

The HSTC focuses on the transnational issues that share one common link – illicit international travel. It brings together federal agency representatives from the policy, law enforcement, intelligence, and diplomatic areas to work together on a full-time basis to convert intelligence into effective law enforcement and diplomatic action. The HSTC prepares strategic reports for U.S. law enforcement and U.S. policy-makers. The HSTC is congressionally mandated to produce an annual report about vulnerabilities in travel systems.

The HSTC also serves as a focal point for international police agencies and provides a mechanism for the exchange of information between the United States and its allies. HSTC is the official point of contact for INTERPOL[151] on trafficking matters for the USG. Members of the HSTC conduct frequent training to law enforcement officials, consular officials, prosecutors and non-governmental organizations, both foreign and domestically.

ICE is a major contributor of personnel to the HSTC. The Center's Director is an ICE employee. The ICE Office of Intelligence provides intelligence support through the Intelligence Program Division's Human Smuggling and Public Safety Unit.

The shortage of staff at the Center has impeded its ability to accomplish its mission. According to the HSTC charter, "[t]he principal determinant of the success of the Center will be its ability to draw on and integrate the diverse experience and perspectives of its full-time staff ... it is critical that key members of the community of interest provide well-qualified personnel to the Center."[152] Various agency members of the community of interest have made commitments to detail personnel to the Center but have been inconsistent in doing so. For example, there are no staff currently detailed to the Center from DOD, FBI, or CIA.

Congress may wish to consider legislatively-mandating minimum staffing by agencies critical to the Center's success. At present, each participating agency provides staff "out of hide," meaning

[150] P.L. 108-458, Dec. 17, 2004, §7202(c), 118 Stat. 3813.

[151] INTERPOL (International Criminal Police Organization) is the world's largest police organization. It assists law enforcement agencies in each of its 187 member countries to combat all forms of transnational crime. See INTERPOL at http://www.interpol.int/public/icpo/default.asp

[152] HSTC, *Charter*, (as amended), Dec 10, 2007, p. 8. The Charter (on p. 2) describes its Community of Interest as "All of the U.S. Government agencies, including missions abroad, having policy, law enforcement, intelligence, diplomatic and/or administrative responsibilities related to migrant smuggling and/or trafficking in persons; the community of interest includes, but is not limited to, the following: (1) the Departments of State, Defense, Homeland Security, Justice and Labor; (2) various federal law enforcement agencies, including the Directorate of Border and Transportation Security, the FBI, USCG, and the Diplomatic Security Service; and (3) several national intelligence agencies, including the CIA and NSA.

they are not reimbursed for the personnel they detail to HSTC. To alleviate this impact, Congress may also wish to consider dedicated funding for the detailee positions at the Center.

U.S. Citizenship and Immigration Services (USCIS) Intelligence Element

As the agency that oversees lawful immigration to the United States, USCIS establishes immigration services, policies and priorities to preserve America's legacy as a nation of immigrants while ensuring that no one is admitted who is a threat to public safety.[153] The Homeland Security Act of 2002 established USCIS as a component of DHS in 2003 and transferred to the new agency the immigration and citizenship adjudication functions of the former INS.[154] The three principal immigrant service activities of USCIS are the adjudication of petitions for immigration benefits; the adjudication of naturalization petitions from lawful permanent residents desiring to become U.S. citizens; and the consideration of refugee and asylum claims, and related humanitarian and international concerns.[155]

USCIS is not a law enforcement agency nor a member of the IC and the vast majority of its funding is derived from fees collected from immigration benefit applicants and petitioners.[156] Thus its activities are limited to adjudication of immigration benefits, which includes conducting background checks on the individuals and organizations who submit applications and petitions, as well as the intended beneficiaries. As part of that process, USCIS collects biometrics, in the form of digital photographs and fingerprints. On average each day, USCIS processes 30,000 applications for immigration benefits, issues 7,300 Permanent Resident Cards (Green Cards), adjudicates 400 refugee applications, and naturalizes 3,400 new civilian citizens and 30 new citizens who are member of the U.S. Armed Forces.[157]

USCIS also has the authority to detect and combat immigration fraud.[158] In a Conference Report to the FY2005 Department of Homeland Security Appropriations Act, Congress recognized USCIS as the responsible agency for developing, implementing, directing, and overseeing the joint USCIS-ICE anti-fraud initiative and conducting law enforcement/background checks on every applicant, beneficiary, and petitioner prior to granting any immigration benefits.[159] Individuals and organizations intent on harming the United States have become increasingly

[153] USCIS, "About Us." http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=2af29c7755cb9010VgnVCM10000045f3d6a1RCRD&vgnextchannel=2af29c7755cb9010VgnVCM10000045f3d6a1RCRD

[154] P.L. 107-296, November 25, 2002, §451, 116 Stat. 2195. See also CRS Report RL33319, *Toward More Effective Immigration Policies: Selected Organizational Issues*, by Ruth Ellen Wasem. The Executive Office for Immigration Review (EOIR), which includes the Immigration Court and the Board of Immigration Appeals, and which reviews decisions made by USCIS, remains under the jurisdiction of the Department of Justice. See EOIR, *Background Information*. http://www.usdoj.gov/eoir/background.htm

[155] CRS Report RL32235, *U.S. Immigration Policy on Permanent Admissions*, by Ruth Ellen Wasem.

[156] In the DHS Appropriations Act of 2010 (P.L. 111-83, Oct. 28, 2009), USCIS received $2,727 million in gross budget authority which consists of $2,503 million in revenue from collected fees and $224 million in direct appropriations. See CRS Report R40642, *Homeland Security Department: FY2010 Appropriations*, coordinated by Jennifer E. Lake and Chad C. Haddal, p. 87.

[157] USCIS Briefing to CRS, Feb. 17, 2010.

[158] See CRS Report RL34007, *Immigration Fraud: Policies, Investigations, and Issues*, by Ruth Ellen Wasem

[159] Conference Report to accompany H.R. 4567 [Report 108-774], "Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2005," p.74.

sophisticated in their methods of gaining entry into the country.[160] The nexus between immigration benefit fraud and threats to national security was illustrated in the 1993 World Trade Center bombing when the plot's mastermind, Mahmud Abouhalima, received a residency visa as an "agricultural worker" despite the fact that he was employed as a New York City cab driver. [161]

In 2004, USCIS established the Office of Fraud Detection and National Security (FDNS). In January 2010, FDNS was promoted to a Directorate to reflect the priority USCIS places on its anti-fraud and national security responsibilities and to place greater emphasis on them. FDNS consists of four branches that collectively are responsible for detecting, pursuing, and deterring fraud; ensuring background checks are conducted on all persons seeking benefits before granting benefits; identifying systemic vulnerabilities and other weaknesses that compromise the integrity of the legal immigration system; and serving as USCIS' primary conduit to and from law enforcement and intelligence agencies. [162]

The USCIS Intelligence Branch

Within FDNS, there is an Intelligence Branch that manages the analysis, reporting, production, and dissemination of immigration-based intelligence products. Those products are designed to focus on the identification of fraud trends or vulnerabilities that are being exploited in the immigration benefits processes while also enhancing national security efforts. The branch manages and directs assets and resources at the headquarters office, five USCIS Service Centers, and within all District Offices. It also establishes liaison with state and local intelligence fusion centers to promote information sharing and collaboration efforts. The branch is also the conduit for information-sharing, coordination, and collaboration with the IC and various law enforcement agencies.

To promote information sharing and provide immigration subject matter expertise, FDNS has placed liaison officers within DHS I&A, the Terrorist Screening Center, NCTC Terrorist Identities Group, the National Joint Terrorism Task Force, DHS Threat Task Force (DTTF),[163] ICE National Security Unit, CBP NTC, State Department's Kentucky Consular Center,[164] FBI National Name Check Program (NNCP),[165] the HSTC, INTERPOL Headquarters in Lyon, France, and the INTERPOL U.S. National Central Bureau.

---

[160] USCIS, USCIS Strategic Plan 2008-2012, p. 7.

[161] Abouhalima applied for the amnesty available to farm workers in 1986 immigration legislation, received temporary legal residence in 1988, and became a lawful permanent resident two years after that. See *Time*, "The Secret Life of Mahmud the Red," Oct. 4, 1993. http://www.time.com/time/magazine/article/0,9171,979338,00.html

[162] USCIS briefing to CRS, Feb. 17, 2010.

[163] The DTTF was established in the summer of 2009 to support high-profile investigations by the FBI. It is composed of I&A analysts and representatives from DHS operational components including USCIS. See Statement for the Record of Caryn Wagner, DHS Under Secretary for Intelligence and Analysis, U.S. Congress, House Committee on Appropriations, Subcommittee on Homeland Security, *DHS Intelligence Programs and the Effectiveness of State and local Fusion Centers*, 111th Cong., 2nd sess., March 4, 2010, p. 6.

[164] The Kentucky Consular Center was established in 2000 by the U.S. Department of State to take over administration of the Diversity Visa Lottery program from the National Visa Center in Portsmouth, New Hampshire. The Diversity Lottery program is an annual lottery run by the State Department which offers up to 55,000 permanent resident visas each year to randomly selected applicants from eligible countries. Source: Department of State, Bureau of Consular Affairs, "Kentucky Consular Center Information." http://travel.state.gov/visa/immigrants/types/types_1321.html

[165] The mission of the NNCP is to disseminate information from FBI files in response to name check requests received from federal agencies; components within the legislative, judicial, and executive branches of the federal government; foreign police and intelligence agencies; and state and local law enforcement agencies within the criminal justice

Intelligence Research Specialists within the branch conduct research and analysis to identify previously unknown links, associations, emerging trends, correlations, anomalies, and indications and warnings with national security or public security threat implications. They produce and disseminate immigration-related intelligence products to a broad audience to include field officers, field and headquarters leadership at USCIS, DHS components, and other Federal, state, and local agencies.[166] For example, there is considerable potential intelligence value in the research and analysis of data within the various USCIS electronic databases as well as the information contained in the more than 90 million immigrant Alien Files (A-Files)[167] in the custody of USCIS (with more than 7 million new A-Files added each year).

An example of the type of intelligence product produced by the FDSN Intelligence Branch was a classified report following the June 2007 failed bombings in London and Glasgow. Police in the United Kingdom (UK) determined that the suspects, who utilized al Qa'ida-like strategies and devices, were immigrants to the UK and working there as medical professionals.[168] This suggested the possibility of similar tactics being used in attacks within the United States. In a response to those events, the FDNS Intelligence Branch queried USCIS databases and records for information on individuals with backgrounds similar to those of the UK plotters. A classified report was produced that identified individuals with exact matches to national security-related hits and individuals under investigation by Federal law enforcement. In addition, over 30 individual intelligence reports were prepared, published, and disseminated to the Intelligence Community.

The Intelligence Branch also administers the USCIS Request for Information (RFI) program, coordinating the preparation of agency responses to requests for immigration information from agencies and organizations outside of DHS, as well as other components and offices within DHS.

Transportation Security Administration (TSA) Intelligence Element

In November 2001, Congress established TSA through the *Aviation and Transportation Security Act of 2001 (ATSA)*.[169] The agency was originally made part of the Department of Transportation, but was transferred to DHS pursuant to the *Homeland Security Act* when the Department was established in March 2003.

TSA is most commonly known for its aviation security role, particularly the security screening of airline passengers and their baggage. However, *ATSA* assigned the Assistant Secretary for TSA responsibility for security in all modes of transportation – aviation, maritime, mass transit, highway and motor carrier, freight rail, and pipeline.[170] These modes form a transportation network that is central to the American economy. That network connects cities, towns, and farms, and moves millions of people and millions of tons of goods. The majority of transportation

system. Source: FBI, "National Name Check Program." http://www.fbi.gov/hq/nationalnamecheck.htm

[166] Ibid.

[167] A-Files are the official immigration records detailing entry and exit of immigrants dating back to the 19th Century. INS began issuing each immigrant an alien registration number in 1940, and on April 1, 1944, began using this number to create individual files, called Alien Files or A-Files. They are a rich source of biographical information and other documentation including immigration documents, visas, photographs, applications, affidavits, correspondence, etc. See USCIS, *FY2007 Annual Report*, p. 95.

[168] The Associated Press, "Suspects held in London, Glasgow Bombings," USA Today, July 3, 2007. http://www.usatoday.com/news/world/2007-07-03-britain-suspects_N.htm

[169] P.L. 107-71, Nov. 19, 2001. Now codified as 49 U.S.C. 114.

[170] 49 U.S.C. 114.(d).

infrastructure in the United States is privately-owned. The remainder is owned and operated by state, local, or regional entities.

The size of the transportation sector in the United States makes it impossible for the Federal government to provide security for all modes. The exception is the commercial aviation sector. But, TSA does provide threat and other intelligence information to support security programs for each sector. In addition, TSA collaborates with industry and government operators and other stakeholders to develop strategies, policies, and programs to reduce security risks and vulnerabilities within each mode. Finally, it seeks to enhance capabilities to detect, deter, and prevent terrorist attacks and respond to and recover from attacks and security incidents, should they occur.

TSA uses a threat-based, risk management approach to the security task. According to former TSA Administrator Kip Hawley: "It begins with intelligence gathered by multiple U.S. agencies that is analyzed, shared, and applied."[171] Intelligence is a key driver in determining the level of security appropriate for the threat environment.

TSA Office of Intelligence (TSA-OI)

The Assistant Secretary for TSA is responsible "to receive, assess, and distribute intelligence information related to transportation security and to assess threats specifically related to transportation.[172] The TSA intelligence function is centered in its Office of Intelligence (TSA-OI) and led by an Assistant Administrator for Intelligence. The office consists of six divisions and an intelligence cell at the Transportation Security Operations Center (TSOC) (also known as the "Freedom Center") in Herndon, Virginia.

TSA-OI Analysis

OI is the only organization that analyzes threats specifically related to transportation. Although it is not an intelligence collector, the office works closely with IC agencies. It participates in NCTC's Daily Intelligence Secure Video Teleconference (SVTS) and receives and analyzes intelligence from the IC to determine its relevant to transportation security. Sources of information outside the IC include other DHS components, law enforcement agencies, and owners and operators of transportation systems. OI also reviews and analyzes the suspicious activity reporting by Transportation Security Officers, Behavior Detection Officers, and the Federal Air Marshal Service (FAMS). The office also works on intelligence issues with its counterparts in the United Kingdom and Canada.

An extensive two-way exchange of information is a unique aspect of OI's relationship with its stakeholders. OI has received funding associated with the Implementing Recommendations of the 9/11 Commission Act of 2007, to establish and implement an information sharing and analysis center (ISAC) [173] for transportation security. OI is in the process of developing both the concept

[171] Kip Hawley, "Aviation Passenger Screening Oversight," Testimony before the U.S. Congress, Senate Committee on Commerce, Science, and Transportation, "Aviation Passenger Screening Oversight," 109th Cong., 2nd sess., *CQ Congressional Testimony*, April 4, 2006.

[172] 49 U.S.C. 114(f).

[173]Establishment of Information Sharing and Analysis Centers (ISAC) was encouraged by Presidential Decision Directive 63 and Homeland Security Presidential Directive (HSPD)-7, to protect infrastructure from attack. ISAC's were set up by and for critical infrastructure owners and operators to provide a trusted, collaborative, information/intelligence sharing and analysis capability. See HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection," Dec. 17, 2003. http://www.fas.org/irp/offdocs/nspd/hspd-7.html

for the TS-ISAC and a milestone plan to establish this capability by early FY2011. Once operational, TSA envisions that the TS-ISAC will provide enhanced solutions for collaboration and information sharing with its stakeholders in the transportation industry.

OI analysts review and analyze information from its many sources in order to produce intelligence on current and emerging threats to U.S. transportation modes, provide tactical support to Federal Air Marshal missions, and support security for other special events. The Intelligence Watch and Outreach Division provides 24/7 indications and warning of threats to the transportation network. The Transportation Intelligence Analysis Division is responsible for in-depth threat analyses. Products are disseminated at appropriate classification levels to OI's principal stakeholders – the TSA leadership, the Office of Security Operations (which performs day-to-day management of the TSA aviation security program), the Office of Global Strategies, Transportation Security Network Management, the FAMS, and public and private transportation industry elements. Intelligence products are also shared with IC members and other DHS organizations.

OI analytic products include the Administrator's Daily Intelligence Brief, Information Bulletins and Circulars, the Transportation Suspicious Incident Reports (TSIR), and the Transportation Intelligence Note (TIN). The TSIR and the TIN products contain information on the latest potential threats, intelligence estimations and trends, and situations observed in transportation systems around the nation and the world. They are produced at the Unclassified/For Official Use Only level for TSA employees and transportation security professionals to enhance situational awareness.

Field Intelligence Officer Program

TSA-OI has deployed field intelligence officers to major airports throughout the United States. They work directly for OI through the respective Eastern or Western Regional Field Intelligence Coordinator. The field intelligence officers are responsible for providing intelligence support and threat briefings to the TSA Federal Security Directors, their staffs, and security workforce in their area of responsibility. In addition, they conduct liaison with the JTTF's and state, local, and tribal law enforcement officials and intelligence fusion centers.

TSA-OI Support to TSA Security Activities

Airline Passenger Pre-Screening

Former TSA Administrator, Kip Hawley has described TSA's aviation security strategy as an interlocking system of multiple layers of security.[174] But, he says, "[w]e cannot focus on a 'catch them in the act" strategy that waits until a person tries to board an aircraft with a weapon ... our success is greatly improved with our ability to anticipate the terrorist act and thwart it well before it gets off the ground."[175] He goes on to say "[a]s important as it is to detect threat objects, it is

[174] U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, *Ensuring America's Security: Cleaning Up the Nation's Watchlists*, Statement of Kip Hawley, Assistant Secretary for TSA, 110th Cong., 2nd sess., Sep. 9, 2008, p. 1. Hereafter: Hawley Statement, Sep. 2008)

[175] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Statement by Kip Hawley, Assistant Secretary of TSA*, 110th Cong., 1st sess., Jan. 17, 2006, p. 3.

imperative that we use intelligence to aid in the identification and interception of the people who would do us harm."[176]

Intelligence supports several elements of the airline passenger prescreening systems in use or proposed by TSA, such as the No Fly and Selectee Lists and Secure Flight. OI's specific role in each of these is described below.

No Fly and Selectee Lists

In addition to uncovering terrorist plots, U.S. intelligence and law enforcement agencies focus considerable effort on identifying individuals who are believed to be or are suspected of being terrorists. Agencies in possession of such intelligence nominate such persons for inclusion in the U.S. Government's consolidated terrorist watchlist, the TSDB. The "No Fly" and "Selectee" lists are subsets of the TSDB that are used to screen air travelers.

The "No Fly" list contains the names of individuals who are prohibited from boarding an aircraft "based on the totality of information, as representing a threat to commit an act of 'international terrorism' or 'domestic terrorism (as defined in 18 U.S.C. 2331) to an aircraft (including threat or air piracy, or a threat to airline, passenger, or civil aviation security), or representing a threat to commit an act of "domestic terrorism" with respect to the homeland."[177]

The "Selectee" List is a list of individuals who "do not meet the criteria to be placed on…the "No Fly" list…and who meet the selectee criteria as members of a foreign or domestic terrorist organization (including foreign terrorist organization designated pursuant to 8 U.S.C. 1189); or associated with terrorist activity (as defined in Section 212(a)(3)(B) of the Immigration and Nationality Act)…"[178] Individuals on the Selectee List may fly only after they and their checked and carry-on baggage have been subjected to additional screening

Originally maintained by TSA (and the FAA prior to 9/11), the No Fly and Selectee lists were transferred to the Terrorist Screening Center (TSC) in 2004. The TSC was established under the auspices of the FBI in an initiative under Homeland Security Presidential Directive (HSPD)-6.[179] These lists are distributed to TSA, which is responsible for screening domestic airline passengers, and CBP which screens international passengers for admittance to the United States. At present, for domestic flights, the matching of passenger names against No Fly and Selectee lists is performed by the airlines on the basis of unclassified versions of watch lists sent to them by TSA.

There has been controversy about the No Fly list—its size and the names of those reported to have been on the list. The American Civil Liberties Union (ACLU) claimed in 2008 that the list contained over 1 million names.[180] Individuals who have been reported at some point to be on the list—and were either refused travel or allowed to travel only after some delay—include politicians, musicians, and figures from other professions.[181] It was even reported that some

[176] Hawley Statement, Sep. 2008, p. 2.

[177] Transportation Security Administration, *Policy Memo, Subject: TSA No Fly and Selectee Lists*, 2005, pp 1-2.

[178] Ibid, p. 3.

[179] HSPD-6, "Integration and Use of Screening Information," September 16, 2003. http://www.fas.org/irp/offdocs/nspd/hspd-6.html

[180] Los Angeles Times, "Terrorist Watch List at Airports Tops 1 Million Names, July 15, 2008. http://latimesblogs.latimes.com/presidentbush/2008/07/terrorist-watch.html

[181] A list of such individuals with footnoted sources is at Wikipedia, "No Fly List: False Positives and Other Controversial Cases." http://en.wikipedia.org/wiki/No_Fly_List

Federal Air Marshals were denied boarding on flights they were assigned to protect because their names matched those on the No Fly list.[182]

The U.S. Government maintains that it has scrubbed these lists. At an October 22, 2008 press conference, then-DHS Secretary Michael Chertoff said there are 2,500 on the No Fly list, fewer than ten percent of whom are U.S. persons. He also said that there are less than 16,000 individuals on the Selectee lists.[183] However, following the attempted bombing of Northwest Flight 253, on December 25, 2009, the No Fly List has nearly doubled to approximately 6,000 according to a senior intelligence official. "The list expanded, in part, to add people associated with al-Qa'ida's Yemen branch and others from Nigeria and Yemen with potential ties to [Umar Farouk] Abdullmuttalab ... " who is alleged to have attempted the bombing of the flight.[184]

DHS has also established a redress mechanism where individuals, who believe their names are on one of the lists in error, may appeal. The program is called DHS Traveler Redress Inquiry Program (DHS TRIP).[185]

The No Fly and Selectee Lists are an integral part of TSA's airline passenger pre-screening system and one of the biggest tools, the agency argues, for keeping dangerous people off aircraft. OI, however, plays a limited role in who is added to these lists since the preponderance of individuals are nominated for inclusion by other core intelligence and law enforcement agencies.[186] However, according to Acting TSA Administrator Gale Rossides, following the attempted bombing of Northwest Flight 253, "DHS is working with our interagency partners to re-evaluate and modify the criteria and process used to build the Terrorist Screening Database (TSDB),[187] including adjusting the process by which names are added to the No-Fly and Selectee Lists."[188]

---

[182] Washington Times, "Air Marshal Names Tagged on No Fly List," Apr. 29, 2008. http://www.washingtontimes.com/news/2008/apr/29/air-marshals-names-tagged-on-no-fly-list/

[183] CNN, "Terrorist Watchlists Shorter than Previously Reported," Oct. 22, 2008. http://www.cnn.com/2008/TRAVEL/10/22/no.fly.lists/index.html

[184] Jillian Coyle, "No Fly List Nearly Doubled After Christmas Incident," *WUSA9.com.* http://www.wusa9.com/rss/local_article.aspx?storyid=98293

[185] The DHS Traveler Redress Inquiry Program (DHS TRIP) is a central gateway to address watch list misidentification issues; and other situations where travelers believe they have faced screening problems at ports of entry, believe they have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at U.S. transportation hubs. See DHS TRIP website at http://www.dhs.gov/xtrvlsec/programs/gc_1169673653081.shtm#1

[186] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *TSA's Office of Intelligence: Progress and Challenges*, Testimony of Bill Gaches, Assistant Administrator, TSA Office of Intelligence, 110th Cong., 1st sess., June 14, 2006.

[187] The TSDB is the single U.S. Government terrorist watchlist database. Prior to 9/11, there were at least a dozen separate watchlists maintained by various agencies. Homeland Security Presidential Directive (HSPD) 6, issued in 2003, directed the Terrorist Screening Center (TSC) to consolidate all U.S. Government watchlist information. The TSC is a multi-agency organization administered by the FBI. It provides subsets of the TSDB (e.g., TSA's "No Fly" list) to U.S. Government screening agencies and provides 24/7 operational support to those agencies to accurately match names within the TSDB and individuals being screened. See Office of the Inspector General Audit Division, *Follow Up Audit of the Terrorist Screening Center*, Department of Justice, Audit Report 07-41, Washington, DC, September 2007, p. i, http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf

[188] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening*, Statement of Gale D. Rossides, Acting Administrator, Transportation Security Administration, 111th Cong., 2nd sess., Mar. 10, 2010, p. 7. Hereafter: Rossides Testimony, 2010.

Secure Flight

After abandoning an effort to establish a follow-on system to the Computerized Passenger Prescreening System (CAPPS), TSA began development of a new system of passenger pre-screening called Secure Flight. In October 2008, TSA announced the issuance of the Secure Flight Final Rule.[189] This would shift pre-departure watch list matching responsibilities from individual aircraft operators to TSA, thus carrying out a recommendation of the 9/11 Commission.

Secure Flight is intended to alleviate the biggest challenge in the application of the No Fly and Selectee list in the passenger prescreening process—the incorrect matching of names on these watchlists with non-threatening passengers whose names are similar.[190] Under Secure Flight, airlines will be required to collect a passenger's full name, date of birth, and gender when making an airline reservation. This additional information is expected to prevent most inconveniences at the airport, and will be particularly important for those individuals with names similar to those on the watch list. Then-TSA Administrator Kip Hawley asserts that "Secure Flight will improve security by maintaining the confidentiality of the government's watch list information while fully protecting passengers' privacy and civil liberties."[191]

Under the Secure Flight program, DHS began transferring responsibility for watch list matching to TSA in 2009, and the transition is targeted for completion by the end of 2010.[192]

Support to the Federal Air Marshal Service (FAMS)

The primary mission of the FAMS is to deter, detect, and defeat hostile acts targeting U.S. air carriers, airports, passengers and crews. The United States first established such a capability in 1968 with the FAA *Sky Marshal* program. That program was enlarged in 1985 and renamed the Federal Air Marshal Service. After 9/11, the program was greatly expanded and, pursuant to *ATSA,* was transferred from FAA to TSA. After DHS was established, the FAMS were briefly part of ICE, but were returned to TSA in 2005 where they remain today.

In addition to their anti-hijacking duties, the FAMS provide support during national emergencies and contingencies, such as Hurricane Katrina and the evacuation of American citizens from Lebanon during the 2006 conflict between Israel and Hezbollah. They also participate in Visible Intermodal Prevention and Response (VIPR) teams which augment security at key transportation facilities in urban areas around the country.[193]

However, the predominant activity for the FAMS is to provide in-flight security for commercial airline flights. Some have questioned the extent of air marshal coverage of such flights. In a March 2008 investigative report, CNN claimed that "of the 28,000 commercial airline flights that take to the skies on an average day in the United States, fewer than 1 percent are protected by on-

[189] DHS Transportation Security Administration, "Secure Flight Program," 73 *Federal Register* 64018 - 54066, October 28, 2008. http://www.tsa.gov/assets/pdf/secureflight_final_rule.pdf

[190] TSA Press Release, "TSA to Assume Watchlist Vetting with Secure Flight Program, Oct. 22, 2008. http://www.tsa.gov/press/releases/2008/1022.shtm

[191] Ibid.

[192] Rossides Testimony, 2010, p. 3.

[193] VIPR teams, which include other TSA and DHS personnel work with local security and law enforcement officials to supplement existing security resources, provide deterrent presence and detection capabilities, and introduce an element of unpredictability to disrupt potential terrorist planning activities. See TSA, "VIPR Teams Enhance Security at Major Local Transportation Facilities." http://www.tsa.gov/press/happenings/vipr_blockisland.shtm

board, armed federal air marshals."[194] TSA insists that the size of the federal air marshal cadre should be classified, as well as the number and itinerary of flights on which they fly, arguing that "we should not tip our hand to terrorists and let them know the mathematical probability of air marshals being on flights they may be interested in taking over or otherwise disrupting."[195] However, TSA has publicly stated that the number is in "the thousands."[196]

In order to determine which flights should be covered by air marshals, TSA uses an intelligence-driven, risk-based approach. This informs FAM deployments during "steady state" threat conditions and in cases of heightened threat, such as in August 2006 after discovery of the Transatlantic Airline Bombing Plot and in December 2009, following the attempted bombing of Northwest Flight 253. OI provides intelligence to support FAMS mission planning and has an intelligence unit, manned 24/7, at the TSOC.

[194] CNN, "Sources: Air marshals missing from almost all flights," Mar. 25, 2008. http://www.cnn.com/2008/TRAVEL/03/25/siu.air.marshals/index.html

[195] TSA, "Federal Air Marshal Shortage?" http://www.tsa.gov/approach/mythbusters/fams_shortage.shtm

[196] Ibid.

The U.S. Coast Guard (USCG) Intelligence Element

As a nation of travelers and traders, America has a strategic interest in the maritime domain.[197] The oceans bordering North America are both a barrier and a highway, separating the United States from potential enemies, connecting it to allies, and providing a venue for commerce and trade.[198] Due to its complex nature and immense size, the maritime domain is recognized as particularly susceptible to exploitation and disruption by individuals, organizations, and States.[199]

The USCG is a military, multi-mission, maritime service that is the "principal Federal agency responsible for safety, security, and stewardship within the maritime domain.[200] These missions are performed in any maritime region where those interests may be at risk, including international waters and America's coasts, ports, and inland waterways.[201] In March 2003, pursuant to the Homeland Security Act, the USCG was transferred from the Department of Transportation to DHS.[202]

The USCG has several diverse missions—national defense, homeland security, maritime safety, and environmental and natural resources stewardship.[203] To accomplish these missions, the USCG has authorities unique within the Federal government. It is both an armed service[204] and the nation's primary maritime law enforcement agency.[205]

Maritime Domain Awareness

One of the Administration's maritime security planning assumptions is that today's complex and ambiguous threats place an even greater premium on knowledge and shared understanding of the maritime domain.[206] This knowledge and shared understanding is termed "maritime domain awareness" and is defined as "the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United

[197] The maritime domain is defined as "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances." National Security Presidential Directive (NSPD) 41/Homeland Security Presidential Directive (HSPD) 13, "Maritime Security Policy," Dec. 21, 2004, p. 2. Hereafter referred to as NSPD-41/HSPD-13.

[198] Commercial ships transport more than 95% of America's non-North American trade by weight and 75% by value. Commodities shipped by sea currently constitute one-fourth of U.S. gross domestic product. Source: Peter Chalk, *The Maritime Dimension of International Security*, (Santa Monica: Rand Corp, 2008), p 35. In 2009, there were 13.5 million cruise line passenger embarkations. Direct spending by cruise lines and their passengers exceeded $19 billion. Source: Cruise Lines International Association, *2010 Cruise Industry Source Book*, p. 9. http://www.cruising.org/sites/default/files/PDF/sourcebook/2010SourceBookFINAL.pdf

[199] NSPD-41/HSPD-13, p. 2.

[200] USCG, *USCG Posture Statement With 2009 Budget in Brief*, Feb. 2008, p. 15.

[201] USCG, *Publication 1*, "U.S. Coast Guard, America's Maritime Guardian," Jan. 1, 2002, pp. 5-6.

[202] P.L. 107-296, §888(b), No. 25, 2002, 116 Stat. 2249.

[203] There are eleven statutorily-mandated USCG mission programs: [203] Under "Safety:" Search and Rescue and Marine Safety. Under "Security:" Ports, Waterways, and Coastal Security; Illegal Drug Interdiction; Undocumented Migrant Interdiction, Defense Readiness, and Other Law Enforcement. Under "Stewardship:" Marine Environmental Protection, Living Marine Resources, Aids to Navigation, and Ice Operations. See USCG, *2008 Budget in Brief and Performance Summary*, Feb. 2007, p. 2.

[204] 14 U.S.C. §1.

[205] 14 U.S.C. §2.

[206] The White House, *National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security*, Oct. 2005, p. 1. Hereafter referred to as *National MDA Plan.* http://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf

States."[207] Since it grants time and distance to detect, deter, interdict, and defeat adversaries,[208] maritime domain awareness has been enshrined as a principal objective of the *National Strategy for Maritime Security*.[209]

The achievement of maritime domain awareness is, therefore, the principal objective of the USCG intelligence program. It is a collaborative effort—especially between the USCG and U.S. Navy[210]—and also with DHS components, such as CBP and ICE, other Federal agencies, and the broader maritime community. Coast Guard intelligence collection begins at the port level and encompasses the entire maritime domain and features maritime surveillance activities by patrol aircraft, unmanned aerial vehicles, shore-based radar, and shipboard sensors including radar and passive electronic surveillance systems.

Coast Guard Intelligence and Criminal Investigations

The mission of the Coast Guard Intelligence and Criminal Investigations is to direct, coordinate, and oversee intelligence and investigative operations and activities that support all USCG objectives. It is a binary organization consisting of two closely linked parts:[211]

- The National Intelligence Element conducts "intelligence activities" as defined in Executive Order 12333 and the *National Security Act of 1947*, including the collection, retention, and dissemination of national intelligence (foreign intelligence and counterintelligence) under those authorities. The National Intelligence Element of the USCG became a statutory member of the IC in December 2001 when Congress amended the *National Security Act of 1947*.[212] The USCG Cryptologic Program is part of the National Intelligence Element.
- The Law Enforcement Intelligence Program describes the collection, retention, and dissemination of information pursuant to USCG law enforcement and regulatory authorities. Persons and components that collect, process, and report law enforcement intelligence, or other information, including those persons performing intelligence functions as a collateral duty, are conducting functions under the Law Enforcement Intelligence Program and are not part of the National Intelligence Element.

Assistant Commandant for Intelligence and Criminal Investigations

The Assistant Commandant for Intelligence and Criminal Investigations oversees the entire USCG intelligence and criminal investigations enterprise, is the senior advisor on intelligence

[207] NSPD-41/HSPD-13, p. 5.

[208] *National MDA Plan*, p. 2.

[209] The White House, *National Strategy for Maritime Security Maritime Security*, Sep. 2005. http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf

[210] In a speech to the 18th Annual Surface Navy Association, Chief of Naval Operations, Admiral Mike Mullen stated that next to the close relationship the Navy shares with the Marine Corps, the Navy's continuing partnership with the USCG is "the single most critical relationship we can possibly have when it comes to securing the maritime domain." See States News Service, "CNO Calls For Closer Navy, Coast Guard Teamwork," Jan. 12, 2006.

[211] USCG, CGICIP briefing to CRS, Oct. 27, 2008.

[212] P.L. 107-108 §105, December 28, 2001. DHS I&A is a member of the IC and the USCG National Intelligence Element is the only subordinate component of DHS that is also a member.

matters to the Commandant of the Coast Guard, and is the Intelligence Community Element Head, previously referred to as the Senior Official of the Intelligence Community for the Coast Guard National Intelligence Element.[213] In this role, the Assistant Commandant is responsible for providing intelligence support to USCG operations.

USCG Cryptologic Program

The Cryptologic Program leverages the USCG's unique access, expertise and capabilities in the maritime environment where other U.S. Government agencies are not often present. This provides opportunities to collect intelligence that supports not only USCG missions, but other national security objectives as well.[214] The USCG describes the mission of its Cryptologic Program as: "inform, warn, and protect Coast Guard, joint, combined, and coalition forces defending national and homeland security interests with timely, focused, and actionable signals intelligence (SIGINT)[215] on adversary disposition, plans, and intent to facilitate tactical, operational, and strategic maritime domain dominance."[216]

Through the Service Cryptologic Component, the USCG provides personnel to the National Security Agency/Central Security Service (NSA/CSS) funded through NSA's Consolidated Cryptologic Program. As part of the USCG's Integrated Deepwater System, tactical cryptologic capability will be installed on the new National Security Cutter[217] and select legacy cutters. This capability should become fully operational in early 2011. The cryptologic systems integrated into the cutters are the same systems used by the U.S. Navy giving the cutters full interoperability with the Navy and, the USCG believes, decrease training and development costs.[218] The USCG sees this capability as the cornerstone of the Global Maritime Intelligence Integration effort.[219]

Coast Guard Counterintelligence Service (CGCIS)

The Coast Guard Counterintelligence Service (CGCIS) helps preserve the operational integrity of the Coast Guard by shielding its operations, personnel, systems, facilities, and information from the intelligence activities of foreign powers, terrorist groups and criminal organizations. CGCIS performs this role through counterintelligence investigations, operations, collection, analysis and production, and Counterintelligence (CI) functional services. CI uses these various aspects to also

[213] USCG Briefing for CRS, Jan. 22, 2010, and Office of the Inspector General, *Survey of DHS Intelligence and Collection and Dissemination*, DHS, OIG-07-49, Washington, DC, June 2007, p. 36. Hereafter referred to as DHS OIG 07-049.

[214] Director of National Intelligence (DNI), *DNI Handbook*, Dec. 15, 2006, p. 26.

[215] As defined in National Security Council Intelligence Directive Number 6 (NSCID 6), SIGINT consists of communications intelligence (COMINT) and Electronic Intelligence (ELINT). COMINT is defined as "technical and intelligence information derived from foreign communications by other than the intended recipients." COMINT activities include the "interception and processing of foreign communications by radio, wire, or other electronic means ... and by the processing of foreign encrypted communications, however transmitted." ELINT is the intelligence produced from "the processing ... of information derived from foreign non-communications [and] electro-magnetic radiation emanating from other than atomic detonation or radioactive sources." Cited in Richelson, *The U.S. Intelligence Community*, p. 31.

[216] USCG, Briefing on the Coast Guard Cryptologic Program to CRS, Oct. 27, 2008.

[217] For background on the National Security Cutter, see CRS Report RL33753, *Coast Guard Deepwater Acquisition Programs: Background, Oversight Issues, and Options for Congress*, by Ronald O'Rourke.

[218] USCG, Briefing on the Coast Guard Cryptologic Program to CRS, Oct. 27, 2008.

[219] The Global Maritime Intelligence Integration Plan is one of several implementation plans directed under NSPD-41/HSPD-13 (pp.5-6). The plan's objective is to integrate all available intelligence regarding threats to U.S. interests in the maritime domain.

provide support to anti-terrorism/force protection; research and technology protection; and infrastructure protection/information operations. CGCIS works with the DHS CI program to ensure interoperability and to provide unique capabilities throughout DHS.

Coast Guard Investigative Service (CGIS)

The mission of the CGIS is to conduct professional criminal investigations, engage in law enforcement information and intelligence collection, provide protective services and establish and maintain law enforcement liaison directed at preserving the integrity of the Coast Guard, protecting the welfare of Coast Guard personnel, and supporting Coast Guard and DHS maritime law enforcement and counter-terrorism missions worldwide. CGIS is a federal law enforcement agency whose authority is derived from 14 U.S.C. §95. This authority provides for USCG special agents to conduct investigations of actual, alleged, or suspected criminal activity; carry firearms; execute and serve warrants; and make arrests within their jurisdiction as defined in the statute.[220]

Other Key USCG Intelligence Organizations

The Coast Guard is divided operationally into two geographic areas, the Atlantic and Pacific. These, in turn, are divided into districts; each of which is responsible for a portion of the nation's coastline. The intelligence elements that support the operational organizations are overseen by the Assistant Commandant. They are the Intelligence Coordination Center, the Atlantic and Pacific Area Intelligence staffs, the Maritime Intelligence Fusion Centers, and the District and Sector Intelligence staffs.

The Coast Guard Intelligence Coordination Center (ICC)

The ICC is the national-level coordinator for collection, analysis, production, and dissemination of Coast Guard intelligence.[221] It is the focal point of interaction with the intelligence components of other government entities such as the Department of Defense and Federal law enforcement agencies at the national level. The ICC is co-located with the U.S. Navy's Office of Naval Intelligence at the National Maritime Intelligence Center in Suitland, Maryland, and supports all Coast Guard missions. The ICC conducts the following activities:[222]

- Manages, analyzes, and produces intelligence that satisfies the unique maritime intelligence requirements of the USCG that include the areas of law enforcement, military readiness, counterterrorism, force protection, marine environmental protection, and port and maritime security.
- Analyzes, produces, and disseminates maritime intelligence in support of senior officials of the USCG, DHS, and other national decision makers.
- Manages the USCG intelligence collection requirements and collections management processes.
- Maintains a 24-hour Indications and Warning Center and current intelligence watch which includes the COASTWATCH Branch.

[220] USCG, Briefing on CGIS to CRS, Jan. 22, 2010.

[221] USCG, CGICIP briefing to CRS, June 30, 2008.

[222] USCG, ICC briefing to CRS, Oct. 27, 2008.

COASTWATCH

The ICC, in conjunction with the Office of Naval Intelligence and CBP, systematically screens arriving commercial vessels for potential security and criminal threats in the form of suspect ships and people. Current regulations require commercial vessels greater than 300 gross tons to submit advanced notice of arrival (NOA) information to the National Vessel Movement Center 96 hours prior to expected arrival in the U.S. ICC *Coastwatch* checks notice of arrival information against federal databases to identify potential security and criminal threats. *Coastwatch's* goal is to provide Coast Guard and interagency decision makers as much advance warning as possible, permitting time to coordinate appropriate operational responses and risk mitigation actions. *Coastwatch* has provided thousands of advanced warnings about arriving individuals identified in Federal counterterrorism, law enforcement, and immigration databases as national security or criminal threats.[27]

Maritime Intelligence Fusion Centers (MIFC)

These centers are analysis and production centers that provide intelligence analysis to USCG operational commanders, the DOD, and IC and other law enforcement partners on geopolitical issues, terrorism, vessel movements and vessels of interest, transnational crimes (drugs, piracy, human smuggling), port security, and living marine resources.[223] The Atlantic MIFC is located in Virginia Beach, Virginia and covers the North and South Atlantic, Gulf of Mexico, Caribbean, Western Mediterranean, and the Great Lakes and all navigable waterways east of the Rocky Mountains. The Pacific MIFC is located in Alameda, California and covers the North, Central, and South Pacific including the Pacific Rim and the west coast of South America.[224]

Area and District Intelligence Staffs

These staffs provide intelligence support to their respective commanders and the International Ship and Port Facility Code (ISPS) Program.[225] District intelligence staffs are also responsible for coordinating human intelligence (HUMINT) collection, conducting regional law enforcement and intelligence liaison, and overseeing the Sector Intelligence Officers.[226]

Sector Intelligence Staffs (SIS).

The SIS is the key intelligence support element for all operations within a Coast Guard Sector. The SIS is led by a Sector Intelligence Office (SIO). The SIO is the primary intelligence advisor to the Sector Commander. Having successfully integrated the Field Intelligence Support Teams (FISTs) into the Sector Intelligence Staff, each Coast Guard Sector now has a full time dedicated maritime intelligence component to provide port-level threat assessments as well as conduct collection and reporting for all Sector wide maritime-related threats. As part of these efforts, they

[223] USCG CGICIP Briefing to CRS, June 30, 2008.

[224] DHS OIG 07-49, p. 39.

[225] In December 2002, contracting states to the 1974 Safety of Life at Sea Convention, met at the International Maritime Organization (IMO) in London, and agreed to a comprehensive security regime for ships and port facilities. This new regime, called the International Ship and Port Facility Security Code (ISPS Code), contains detailed security-related requirements for Governments, port authorities, and shipping companies (Part A), together with a series of guidelines about how to meet these requirements (Part B).

[226] USCG, CGICIP briefing to CRS, June 30, 2008.

conduct liaison with Federal, state, local, tribal, and industry partners.[227] The SIS' also report on activities in foreign ports by debriefing ship crews that have returned to the United States from overseas. These interviews are used at the ICC and the MIFC's to identify vessels or individuals of interest arriving at U.S. ports, or potential threats to maritime security.[228]

U.S. Secret Service (USSS) Protective Intelligence and Assessment Division

Although the USSS[229] is best known for its responsibility to protect the President and Vice President of the United States and visiting foreign heads of state and government, it was first established in 1865 as a law enforcement agency with a mandate to investigate the counterfeiting of U.S. currency. Its protective responsibilities began in 1901 following the assassination of President McKinley and were codified by Congress in 1906. The USSS remained a distinct organization within the Department of the Treasury until its transfer to DHS effective March 1, 2003, pursuant to the Homeland Security Act of 2002.[230]

Today, in addition to its protective service mission, the USSS is responsible for maintaining the integrity of the nation's financial infrastructure and payment systems. This was historically accomplished through the enforcement of counterfeiting statutes, but since 1984, its investigative responsibilities have expanded to include crimes that involve financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, electronic funds transfers, and certain money laundering crimes.[231]

USSS Organizational Structure

The USSS employs approximately 3,500 special agents, 1,350 Uniformed Division officers, and more than 1,800 other technical, professional, and administrative support personnel. They work at the headquarters in Washington, D.C. and in 142 field offices and units within the United States and its territories and 22 offices in 18 foreign countries.[232] The USSS is organized into seven offices, Investigations, Protective Operations, Protective Research, Professional Responsibility, Government and Public Affairs, Human Resources and Training, and Administration. The two principal operational offices are Investigations and Protective Operations. The principal support office from an intelligence perspective is the Office of Protective Research.

---

[227] USCG, Briefing to CRS, Nov. 14, 2008.

[228] DHS OIG 07-49, pp. 40-41.

[229] For a full discussion of USSS missions, see CRS Report RL34603, *The U.S. Secret Service: An Examination and Analysis of Its Evolving Missions*, by Shawn Reese.

[230] P.L. 107-296, § 821, Nov. 25, 2002, 116 Stat. 2224.

[231] Specifically, these crimes include the counterfeiting of U.S. currency (to include coins), foreign currency (occurring domestically), U.S. Treasury checks, Department of Agriculture food coupons, and U.S. postage stamps; identity crimes such as access device fraud, identity theft, false identification fraud, bank fraud and check fraud; telemarketing fraud; telecommunications fraud (cellular and hard wire); computer fraud; fraud targeting automated payment systems and teller machines; direct deposit fraud; investigations of forgery, uttering, alterations, false impersonations or false claims involving U.S. Treasury Checks, U.S. Saving Bonds, U.S. Treasury Notes, Bonds and Bills; electronic funds transfer including Treasury disbursements and fraud within the Treasury payment systems; Federal Deposit Insurance Corporation investigations; Farm Credit Administration violations; and fictitious or fraudulent commercial instruments and foreign securities. Source: USSS website, "Criminal Investigations." http://www.secretservice.gov/criminal.shtml

[232] USSS Briefing for CRS, Jan. 20, 2010.

- Investigations. This office investigates counterfeiting and other crimes against the integrity of the nation's financial infrastructure and payment systems.[233]
- Protective Operations. This office performs the protective service mission of the USSS. Protectees include the President and Vice-President and their families, visiting heads of state and government, major Presidential candidates, and former President and Vice Presidents.[234] It also has a uniformed division that is responsible for security at the White House Complex; the Vice President's residence; the Department of the Treasury (as part of the White House Complex); and foreign diplomatic missions in the Washington, D.C., area. In addition, the Office of Protective Operations executes the USSS's responsibility as the U.S. Government lead agency for planning, coordinating, and implementing the operational security plans for National Special Security Events (NSSE).[235]
- Protective Research. This office is responsible for protective intelligence and analysis. It also evaluates and implements technology-based protective countermeasures. Within its Protective Intelligence and Assessment Division, intelligence, law enforcement, and other information is reviewed and threat and vulnerability assessments are produced.

Protective Intelligence and Assessment Division (PID)

The PID supports the USSS protective service mission through three primary means: (a) receive, evaluate, disseminate, and maintain information concerning subjects (individuals and groups) and activities that pose a known, potential, or perceived threat to persons, property, and events protected by the USSS; (b) investigate those subjects and activities; and (c) conduct protective intelligence 'advances' preceding protectee travel.[236] The division is organized into foreign and domestic branches, a 24-hour duty desk to collect and process threat information, and the National Threat Assessment Center.

Unlike other DHS components that collect as well as analyze and disseminate intelligence information, the USSS is principally a *consumer* of intelligence which it analyzes to mitigate threats to those it is charged to protect. Because of its unique statutory authorities to use intelligence to prevent attacks on the nation's leaders and visiting foreign dignitaries, the USSS maintains that comparisons with intelligence gathering organizations within the IC are difficult, if not impossible.[237]

[233] USSS authority to investigate such crimes is contained in Title 18, U.S.C. §3056(b).

[234] The complete list of statutorily-authorized protectees is in Title 18, U.S.C. §3056(a).

[235] NSSE's are events of national significance that the President or the Secretary of Homeland Security determine warrant special security planning and coordination. According to DHS, "A number of factors are taken into consideration when designating an event as an NSSE, including anticipated attendance by dignitaries and the size and significance of the event. When an event is designated an NSSE, the USSS assumes its legally mandated role as the lead federal agency for the design and implementation of the operational security plan. Federal resources will be deployed to maintain the level of security needed for the event." DHS Press Release, Jan. 28, 2008. http://www.dhs.gov/xnews/releases/pr_1201541187429.shtm. For a thorough discussion of NSSE's, see CRS Report RS22754, *National Special Security Events*, by Shawn Reese.

[236] The White House, ExpectMore.gov, "Secret Service: Protective Intelligence Assessment," Section 1, Number 1.1, Jan. 9, 2009. http://www.whitehouse.gov/omb/expectmore/detail/10002412.2004.html

[237] Ibid.

National Threat Assessment Center (NTAC)[238]

NTAC uses historical information, investigative records, interviews, and other primary source material to produce long-term behavioral research studies that leverage USSS expertise in the protection of persons for homeland security or public safety purposes. The premise for NTAC was developed in the wake of an original assassination research study, the Exceptional Case Study Project (ECSP), conducted in collaboration with the Department of Justice. The ECSP was a study of individuals who had assassinated, attacked, or approached with lethal means, public officials or public figures from 1949-1996 in the United States. One major product from this study was a guidebook on protective intelligence and threat assessment investigations.[239]

The NTAC was then established in 1998 as an effort to dedicate resources to better understand, and find ways to prevent, targeted violence; to share this knowledge with others; and to continue to provide leadership in the field of threat assessment. Through the *Presidential Threat Protection Act of 2000,* Congress formally authorized NTAC to provide assistance to Federal, state, and local law enforcement, and others with protective responsibilities, on training in the area of threat assessment; consultation on complex threat assessment cases or plans; and research on threat assessment and the prevention of targeted violence.[240]

Notable NTAC Research Projects include

- Safe School Initiative (1999-2001). In collaboration with the Department of Education, NTAC studied 37 school shootings, involving 41 attackers that occurred in the United States between January 1974-May 2000. The study examined the thinking, behaviors, and communications of the students who planned and carried out these incidents.[241]
- The Insider Threat Study (2002-08). With financial support from DHS, NTAC partnered with CERT at Carnegie Mellon University, to examine organizational employees who perpetrated harm to their organizations via a computer or system or network to include intellectual property theft, fraud, and acts of sabotage. Four reports were published based on this study.[242]
- Bystander Study (2004-08). In collaboration with the Department of Education and McLean Hospital, NTAC explored how students with prior knowledge of targeted school-based violence made decisions regarding whether and with whom to share the information. A report, *Prior Knowledge of Potential School-based*

[238] USSS briefing for CRS on Oct. 8, 2008.

[239] Robert A. Fein and Bryan Vossekuil, *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials*, (Washington, DC: U.S. Department of Justice, National Institute of Justice, July 1999).

[240] P.L. 106-544, December 19, 2000, §4, 114 Stat. 2716.

[241] The publications include the Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States (2002); Threat Assessment in Schools: A Guide to Managing Threatening Situations and Creating Safe School Climates (2002); and an interactive CD-ROM designed to help threat assessment teams, A Safe School and Threat Assessment Experience: Scenarios Exploring the Findings of the Safe School Initiative (2006).

[242] This study produced four reports, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors (2005); Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector (2006); Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector (2008); and Insider Threat Study: Illicit Cyber Activity in the Government Sector (2008).

Violence: Information Students Learn May Prevent a Targeted Attack, was published in May 2008.

- Institutions of Higher Education Targeted Violence Study (ongoing): Pursuant to a recommendation in a report to the President following the April 2007 shootings at Virginia Tech, [243] the NTAC is in the initial stages of a collaborative project with the Department of Education and the FBI Behavioral Analysis Unit to research targeted violence at institutions of higher education.

Oversight Challenges and Options for Congress

Managing competing claims for intelligence support is one of the biggest challenge facing the DHS IE. Former Under Secretary Allen stressed the importance of supporting the Department itself—both headquarters and operational components—noting that "... keeping dangerous people and dangerous items from crossing our air, land, and sea borders and protecting our critical infrastructures ... requires having reliable, real-time information and intelligence to allow the Department to identify and characterize threats uniformly, support security countermeasures, and achieve unity of effort in the response."[244]

But, the DHS IE also has responsibilities to support the President, the Secretary, and other national leaders with a strategic perspective on a range of "all hazards" homeland security issues including terrorism threats. State, local, and tribal, law enforcement and security officials, as well as the operators of the nation's critical infrastructure, are also important customers. They require timely and actionable intelligence through usable products in order to prepare for and respond to a variety of threats.

Helping the Department achieve the right balance among these competing claims on its intelligence resources and capabilities is a challenging task for Congress. The following are options the Congress may wish to consider in exercising its oversight responsibility.

Support to State and Local Fusion Centers

Joint Fusion Center Program Management Office (JFC PMO)

In 2009, Secretary Napolitano directed I&A to outline a Department-wide initiative to strengthen the baseline capabilities and analytic capacity of state and major urban area fusion centers. As a result, a new program office for the fusion center program, the JFC PMO, will be established. DHS intends for the office to be managed on a day-to-day basis by I&A, but all relevant DHS components will be involved to include staff from those components.[245] Among the intended responsibilities of the new JFC PMO are:

- Lead a unified Department-wide effort to develop and implement survey tools to ensure state, local and tribal customers are provided the opportunities to define and identify the types of homeland security-related information they need, and the format in which they need it.

[243] U.S. Departments of Health and Human Services, Education, and Justice, *Report to the President on Issues Raised by the Virginia Tech Tragedy*, June 13, 2007, p. 9. http://www.hhs.gov/vtreport.html

[244] Allen Testimony, Sep. 24, 2008.

[245] Johnson Testimony, Sep. 24, 2009, p. 6.

- Develop mechanisms, in coordination with federal, state, local, tribal, and territorial authorities, to improve the capability of fusion centers to gather, assess, analyze, and share locally generated and national information and intelligence, in order to provide complete pictures of regional and national threats and trends.[246]

The Secretary requested a recommendation by March 2010 on the feasibility and optimal structure and resources of the JFC-PMO. Under Secretary Wagner has testified that the Department is also considering how a pending JFC-PMO will align with the White House's direction that DHS, in coordination with the PM-ISE, be the lead agency in establishing a National Fusion Center Program Office.[247] The establishment and operation of these offices will be of interest to Congress.

Sustainment Funding

Law enforcement officers have praised fusion centers as a vital resource for information sharing and coordination while at the same time expressing great concern about the sustainment of these centers through consistent funding.[248] Currently, funds from the State Homeland Security Grant Program (SHSGP) and Urban Area Security Initiative (UASI) are used to support state and local fusion centers. These grant programs are managed within DHS by the Federal Emergency Management Agency (FEMA) Grant Programs Directorate (GPD).[249] However, the intelligence and information sharing activities that these funds support are operationally managed by DHS I&A. Some contend this disconnect between fund administration and implementation is problematic.

Congress may wish to consider alternative funding arrangements for fusion centers. One option is to designate a percentage of SHSGP and UASI funds for fusion centers. Another is to authorize and appropriate funding for a new grant program for fusion centers.

Information Technology Infrastructure

The success of the fusion center program is dependent on the infrastructure that enables state and local fusion centers to have access to each other's information as well as to the appropriate federal databases.[250] The fusion center program and the Nationwide Suspicious Activity Report Initiative (NSI)[251] rely on the concept of shared space architecture, where the fusion centers replicate data from their systems to an external server under their control, making the decision on what to share totally under their control. A secure portal is then created that allows simultaneous searching of all such databases so that fusion centers will be able to aggregate any relevant information that exists throughout the national fusion center network. The NSI project team has arranged for secure access to this portal on one of three existing networks—Law Enforcement

[246] Ibid

[247] Wagner Testimony, Mar. 4, 2010. p. 3.

[248] These issues were raised most recently at U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *The Future of Fusion Centers: Potential Promise and Dangers.*111th Cong., 1st sess., Apr. 1, 2009.

[249] For a full discussion of DHS assistance to state and local governments, see CRS Report R40246, *Department of Homeland Security Assistance to States and Localities: A Summary and Issues for the 111th Congress*, by Shawn Reese.

[250] The author is grateful to Paul Wormeli, Executive Director of the IJIS Institute, for his advice on fusion center information technology infrastructure requirements.

[251] For more information on the NSI, see CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Mark A. Randol.

Online, Regional Information Sharing Services, or HSIN. Each fusion center will require a server and software to translate data from whatever case management or intelligence system is in place to a separate database on the server.

Achieving information sharing objectives also requires that partners establish wide-scale electronic trust between the caretakers of sensitive information and those who need and are authorized to use that information. Fusion Centers must, therefore, acquire a federated capability for identity and privilege management that securely communicates a user's roles, rights, and privileges to ensure network security and privacy protections. The two elements of this are identification/authentication—the identity of end users and how they were authenticated; and privilege management—the certifications, clearances, job functions, and organizational affiliations associated with end users that serve as the basis for authorization decisions.[252]

Congress may wish to consider providing funding and leadership to provide this infrastructure capability to all 72 fusion centers.

Quadrennial Homeland Security Review (QHSR)

In February 2010, DHS produced its first Quadrennial Homeland Security Review (QHSR),[253] a comprehensive assessment outlining its long-term strategy and priorities for homeland security and guidance on the Department's programs, assets, capabilities, budget, policies, and authorities. The QHSR report outlines the Nation's homeland security missions, which it describes as *enterprise-wide* (i.e., not limited to DHS):[254]

- Mission 1. Preventing Terrorism and Enhancing Security
- Mission 2: Securing and Managing our Borders
- Mission 3, Enforcing and Administering Our Immigration Laws
- Mission 4: Safeguarding and Securing Cyberspace
- Mission 5: Ensuring Resilience to Disasters

The report also calls for the maturing and strengthening of the homeland security enterprise by:[255]

- Establishing a comprehensive system for building and sharing awareness of risks and threats.
- Developing and implementing a methodology to conduct national-level homeland security risk assessments.
- Enhancing critical tools and institutionalizing arrangements for timely access and effective sharing of information and analysis.
- Establishing a robust approach to identify verification that safeguards individual privacy and civil rights.
- Ensuring shared situational awareness in the air, land and maritime domains.

[252] For details on the Global Federated Identity Management framework which provides a standards-based approach for implementing federated identity, see DOJ, Office of Justice Programs, Justice Information Sharing, "Security and Federated Identity Management." http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1179

[253] The requirement for DHS to produce a QHSR is contained in §2401(a) of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, P.L. 110-53, Aug. 3, 2007.

[254] DHS *QHSR Report*, p. x.

[255] Ibid, pp. 65-75.

- Using and integrating counterintelligence in all aspects of homeland security to thwart attacks against the homeland.
- Promoting a common understanding of security as a shared responsibility.
- Fostering communities that have information, capabilities, and resources to prevent threats, respond to disruptions, and ensure their own well-being.
- Fostering a broad national culture of cooperation and mutual aid.
- Ensuring scientifically informed analysis and decisions are coupled to innovative and effective technological solutions.

A review of the QHSR report and the forthcoming "bottom-up review" will give Congress an opportunity to review the department's latest judgments about the homeland security-related risks facing the country and what resources should be committed to address those risks. The results of that review will be particularly important as Congress considers an authorization bill for DHS.

Evolving Risks

Former Secretary Chertoff has said that "DHS must base its work on priorities that are driven by risk."[256] DHS has defined "risk" as the product of three variables, threat (the likelihood of an attack occurring), vulnerability (the relative exposure to an attack), and consequence (the expected impact of an attack).[257] The DHS IE identifies, measures, and monitors the threat variable in the DHS risk equation.

The role of the DHS IE in risk management decision making at the Department is another area Congress may wish to explore. A recent study by the Homeland Security Institute noted that DHS risk assessments require threat inputs but generating useful threat judgments is challenging.[258] It suggested ways to improve risk and intelligence analyst collaboration to better support DHS decision making.

Terrorism remains the paramount concern to the Department. The latest National Intelligence Estimate on the terrorist threat to the United States, concludes that "Al Qa'ida is and will remain the most serious terrorist threat to the Homeland ... has protected or regenerated key elements of its Homeland attack capability ... and that in its Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population."[259]

Following the hijacking of aircraft, that were then flown into the World Trade Center and the Pentagon with devastating effects, a significant portion of homeland security resources in the United States were understandably devoted to aviation security—an amount proportionally larger than that of other transportation modes or critical infrastructure. The 2006 Transatlantic Airlines Plot and the Christmas Day 2010 attempted bombing of Northwest Flight 253, demonstrate that the threat to commercial aviation remains but that the tactics employed have evolved.

Since 9/11, al-Qa'ida and other terrorist groups with anti-Western and anti-American ideologies have committed several other deadly terrorist attacks, including:

[256] Chertoff, "Second Stage Review Remarks."

[257] DHS, *FY2010 Homeland Security Grant Program: Program Guidance and Application Kit*, Dec. 2009, p. 4.

[258] Homeland Security Institute, *Risk and Intelligence Communities Collaborative Framework*, April 2009.

[259] National Intelligence Council, *National Intelligence Estimate: The Terrorist Threat to the U.S. Homeland*, July 2007, "Key Judgments."

- Bali, 2002. The Islamist group Jemaah Islamiyah bombed nightclubs killing 202.
- Madrid, 2004. A Muslim, al-Qa'ida-inspired terrorist cell bombed commuter trains killing 190 and injuring over 1,000.
- London, 2005. British Islamist extremists bombed city buses killing 52 and injuring over 700.
- Mumbai, 2008. A team from the militant group Lashkar-e-Taiba conducted a shooting and bombing rampage at two hotels, a railway station, hospital, Jewish Center, cafe, and cinema. 164 were killed.

All of these attacks involved mass casualties. All resulted in visually dramatic destruction. But, none of them were committed against civil aviation. Recognizing that some elements of the nation's critical infrastructure are defended in depth against attack, while others are not, a question of abiding interest is whether terrorists might adapt by choosing to attack softer targets in the Homeland, such as nightclubs, commuter trains, buses, or other places where large numbers of Americans congregate.

In addition, in a period of less than one year (May 2009-March 2010), there were 12 "homegrown" jihadist-inspired terrorist attacks and plots (two attacks and 10 plots) by American citizens or lawful permanent residents of the United States. By comparison, in over seven years from the 9/11 attacks through May 2009, there was an annual average of only two such plots, none of which resulted in attacks. This has not gone unnoticed by many who are concerned that domestic radicalization, previously viewed as a problem largely confined to Europe, is a bigger threat in the United States than originally believed.

And what about methods of attack not yet imagined? The Australian scholar Mervyn Bendle asks us to consider one such scenario. The recent catastrophic bushfires in his own country "alert us to the extreme danger posed by pyroterrorism, especially as global terrorist organizations continue to modify their strategies in the face of increasingly effective counterterrorism measures employed against them. Pyroterrorism can do great harm to valuable natural resources and infrastructure; destabilise and degrade regional economies; kill, maim, terrorise, and radically reduce the quality of life of large populations of people; and even destabilise social and political systems." [260]

Bendle argues that this is not an "alarmist, eccentric, or "Islamophobic" notion." His study documents that pyroterrorism involvement has been suspected or established in Greece, Israel, Spain, and Estonia. Moreover, in the late 1990's, the Earth Liberation Front set fire to various forests, commercial and industrial buildings in the United States including the U.S. Forest Service Headquarters in Oregon. [261]

Pyroterrorism is just one example of many alternative hypotheses that homeland security risk managers may wish to consider in order to avoid what was famously described in the *9/11 Commission Report* as "a failure of imagination."[262] Threat assessment is a critical component of the risk equation. Risk, in turn, is an important element of the QHSR which will ultimately inform how the department proposes to allocate resources in the future based on the evolving threat environment.

Therefore, Congress may wish to explore:

[260] Mervyn F. Bendle, "Australia's Nightmare: Bushfire Jihad and Pyroterrorism," *National Observer*, No. 79, Summer 2008/09, p. 8.

[261] Ibid, p. 17.

[262] *9/11 Commission Report*, p. 339.

- How I&A will support the next step in the Department's QHSR process, the top-to-bottom review that is intended to link strategy to program to budget.
- How intelligence analysis and assessments are used within the Department to determine priorities for funding of new or existing homeland security programs.
- How intelligence analyses and assessments have led to increased or decreased funding for existing programs.
- The framework that DHS will establish for enhanced collaboration among risk and intelligence analysts.

Author Information

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism

Acknowledgments

Mark A. Randol, former CRS Specialist in Domestic Intelligence and Counter-Terrorism, was the original author of this report.

Disclaimer