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

Mark A. Randol
Specialist in Domestic Intelligence and Counter-Terrorism

May 27, 2009

Congressional Research Service
7-5700
www.crs.gov
R40602

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

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." 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.

Congress made information sharing a top priority of the Department's intelligence component in the Homeland Security Act of 2002 and underscored that 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.

At the outset of the new Administration, the DHS Intelligence (DHSI) enterprise 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).

As the Obama Administration fills key positions within DHS and I&A, Congress will likely be interested in the progress of integration of the Department's intelligence components and the quality and relevance of the intelligence DHSI produces for front line law enforcement and security officials who are responsible for protecting America and its people. In addition, this year, the Department will produce its first Quadrennial Homeland Security Review (QHSR), a comprehensive assessment that outlines its long-term strategy and priorities for homeland security and guidance on the Department's programs, assets, capabilities, budget, policies, and authorities. The results of the QHSR will be particularly important as Congress considers an authorization bill for the Department.

This report provides an overview of DHSI both at headquarters and within the components. It examines how DHSI is organized and 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 also discusses several oversight challenges and options that Congress may consider on certain issues. This report may be updated.

Contents

Figures

Contacts

Introduction

A 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.[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

[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.

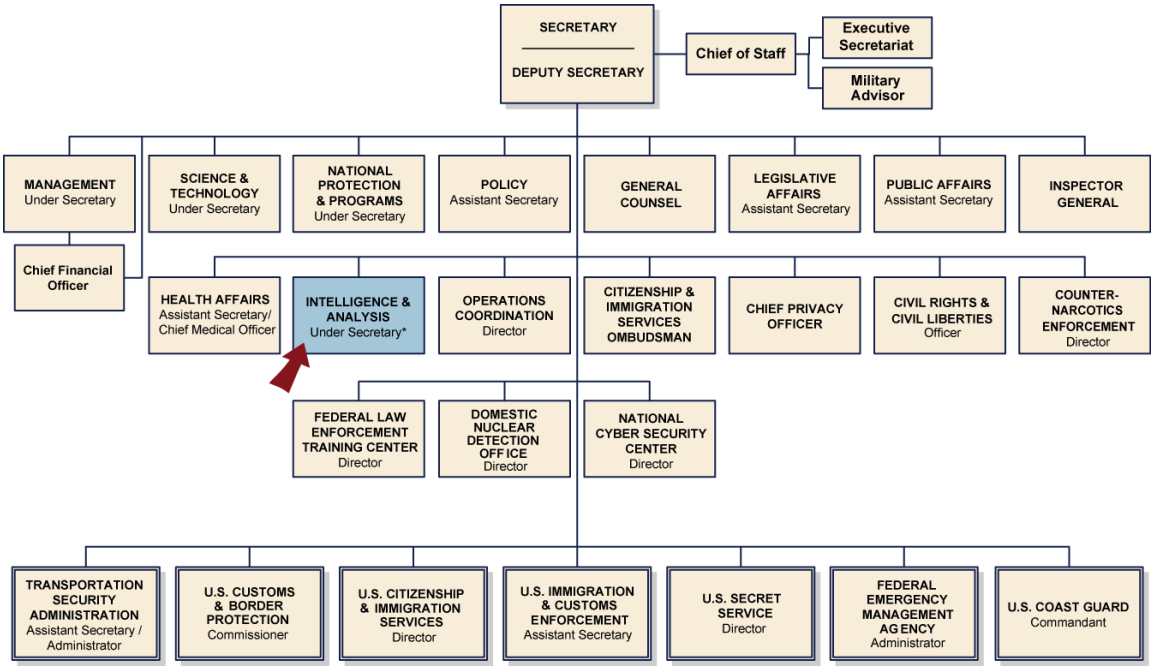
[6] Ibid, §1016b(1), 118 STAT. 3665.

[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."

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 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]

[9] Ibid.

[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.

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

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 DHSI enterprise consists of those elements within DHS that have an intelligence mission. At the outset of the new Administration, it consists of 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

[12] Ibid.

[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.

Administration (TSA), U.S. Coast Guard (USCG), and U.S. Secret Service (USSS). The Department and USCG are statutory members of the IC. [21]

As the Obama Administration fills key positions within DHS and I&A, Congress will likely be interested in the progress of integration of the Department's intelligence components and the quality and relevance of the intelligence DHSI produces for front line law enforcement and security officials who are responsible for protecting America and its people. In addition, this year, the Department will produce its first Quadrennial Homeland Security Review (QHSR), a comprehensive assessment that outlines its long-term strategy and priorities for homeland security and guidance on the Department's programs, assets, capabilities, budget, policies, and authorities. The results of the QHSR will be particularly important as Congress considers an authorization bill for the Department.

Some have argued that there is a broad homeland security intelligence enterprise that encompasses not only DHSI, 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 DHSI 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 Congressional oversight challenges and options concerning certain issues.

Office of Intelligence and Analysis (I&A)

The Homeland Security Intelligence Mission

The mission of I&A is to "ensure 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."[22] The Under Secretary for I&A is the Chief Intelligence Officer for the Department and is responsible to lead I&A and the entire DHSI enterprise. 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.[23]

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."[24] It is an iterative process in which

[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).

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

[23] 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*.

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

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. [25] 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.... [26]

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.[27] 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.'[28]

I&A Customers

I&A's "customer set" is broad. Former Under Secretary Charles Allen saw the Department—both headquarters and the operational components—as I&A's primary customer. "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."[29] Accordingly, I&A's DHS customers range from the Secretary of Homeland Security all the way to individual border patrol agents, Coast Guard seamen, and airport screeners.

(...continued)

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

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

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

[27] 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.

[28] 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).

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

I&A is also 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)[30] Executive Committee. I&A contributes analytic staff to the National Counterterrorism Center (NCTC).

The office also contributes items to the President's Daily Brief[31] providing a homeland security perspective on terrorism and other threats to the United States to the nation's leaders.

State, local, and tribal law enforcement—often described as the "first preventers" of terrorism—are another important set of customers. They 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. Finally, I&A is charged with supporting 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.

Integrating the DHSI Enterprise

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."[32]

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.[33] The HSIC was established to serve as the mechanism to provide senior-level direction for Department-wide

[30] 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.

[31] 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

[32] 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.

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

intelligence activities and to promote integration efforts. It is chaired by the Under Secretary and is comprised of the heads of the DHS component intelligence offices.

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; Tactical Intelligence and Related Activities, which covers programs supporting the operating units of the armed services; and the Joint Military Intelligence Program, which covers programs, not-necessarily tactical, that are of primary concern to the Department of Defense (DOD). Only a small part of the U.S. Government intelligence budget is made public.[34]

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.[35] Those budgets are listed within each component's appropriation, however they are generally co-mingled with other operational activities.[36] 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.[37]

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 and is supported by a Principal Deputy Under Secretary. The current I&A organization is at **Figure 2.**

Office of the Deputy Under Secretary for Intelligence (DU/S-I)

The DU/S-I is responsible for the analytic mission of I&A. The office has been focused on five "analytic thrusts" aligned with the principal threats to the Homeland:[38] 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.

[34] 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

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

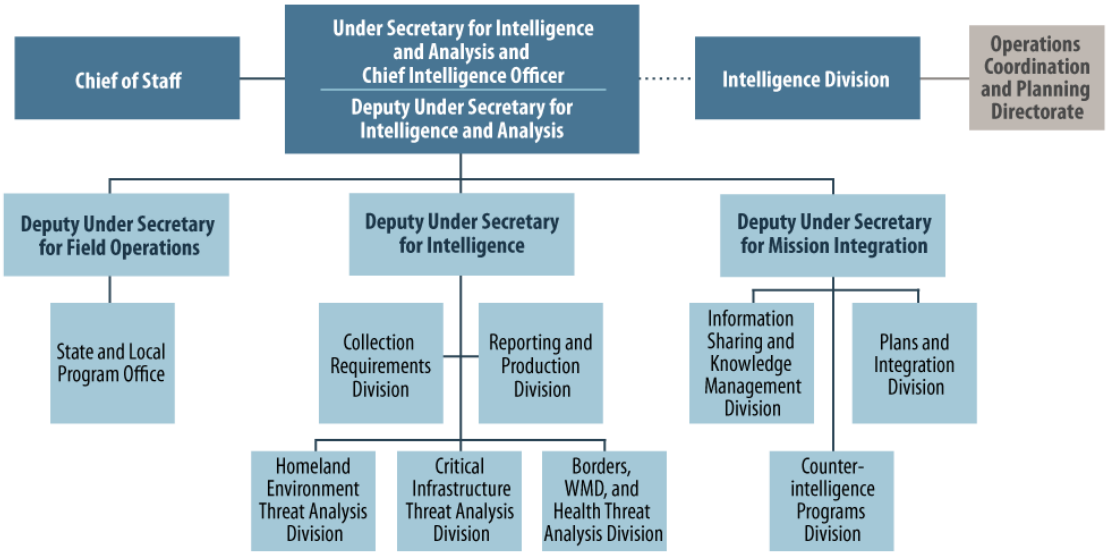
[36] See CRS Report RL34482, *Homeland Security Department: FY2009 Appropriations*, coordinated by Jennifer E. Lake and Blas Nuñez-Neto.

[37] Ibid, Table 6, p. 14. See also OMB: *USG FY10 Budget*, pp. 506-7.

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

There are five divisions within the DU/S-I organization that are engaged in the analytic effort.[39] The Homeland Environment Threat Analysis Division identifies and assesses major threats originating from demographic instabilities, domestic and international radicalization, and future strategic future threats for which DHS must prepare and respond. The Critical Infrastructure Threat Analysis Division integrates all source intelligence from the IC with information from critical infrastructure owners and operators, and, collaboratively with state and local intelligence fusion centers to provide a comprehensive tactical and strategic understanding of physical and cyber threats to the critical infrastructure, including threats from nation-states, international and domestic terrorism, and criminal enterprises.

Figure 2. Office of Intelligence and Analysis Organizational Chart



Source: DHS I&A, March 2009.

The Borders, WMD, and Health Threat Analysis Division monitors, assesses, and reports the threats posed to U.S. borders and to the U.S. population by dangerous people and dangerous things. The Borders branch of this division not only tracks terrorists, but also special interest aliens, transnational gangs such as alien smugglers and narcotics traffickers and how they move their money.[40]

The Collection Requirements Division is the focal point for all collection requirements in an effort to ensure that the intelligence needs of DHS components and customers are articulated, clarified, assigned, and fulfilled. This division represents DHS at IC collection requirement committees. It also manages the DHS Open Source Program which produces domestic open

[39] DHS, Office of Intelligence and Analysis Organizational Chart (with descriptions), Mar. 2009.

[40] U.S. Congress, House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, *A Report Card on Homeland Security Information Sharing*, Testimony of Charles E. Allen, DHS Under Secretary for I&A, 110th Cong., 2nd sess., September 24, 2008. Hereafter: Allen Testimony, Sep. 24, 2008.

source intelligence (OSINT).[41] The Reporting and Production Division integrates DHS and state and local law enforcement information into the IC through Homeland Intelligence Reports. It is also the single point of service across DHSI for state, local, and tribal support requests as well as the central point for dissemination of I&A's finished products.

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.[42] 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 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.

[41] OSINT is the "acquisition of any verbal, written, or electronically transmitted material that can be legally acquired; this includes newspapers, magazines, unclassified journals, conference papers and preprints of articles,, as well as the broadcasts of public radio and television stations and various material appearing on the internet." Richelson, *The U.S. Intelligence Community*, p. 317. The collection of foreign open source material is the responsibility of the DNI Open Source Center. For further information on OSINT, see CRS Report RL34270, *Open Source Intelligence (OSINT): Issues for Congress*, by Richard A. Best Jr. and Alfred Cumming. For a review of the progress by DHS to harness OSINT to enhance information sharing, see U.S. Congress, House Committee on Homeland Security, *Giving Voice to Open Source Stakeholders: A Survey of State, Local & Tribal Law Enforcement*, Report Prepared by the Majority Staff, 110th Cong., 2nd sess, Sep. 2008.

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

- *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)[43] 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:[44] 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.[45] It provides real-time, interactive connectivity between states and major urban areas and the National Operations Center (NOC).[46]

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.[47] I&A has deployed HSDN

[43] 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*.

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

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

[46] 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.

[47] 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 more than 30 state and local fusion centers and intends to install terminals in all of the fusion centers as soon as security requirements are met.[48]

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

There has been some criticism about the focus of I&A analysis and the relevance of its products to state, local, tribal, and private sector customers. 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 ... '"[49] However, later in 2008, state and local officials interviewed by CRS for this report expressed the general view that although this critique may have been true a couple of years ago, it was not true now.[50]

In 2006, former Under Secretary Allen established a State and Local Fusion Center (SLFC) Pilot Project Team to work with six fusion centers[51] in five states to enhance DHS support. At the outset, the team "found a substantial gap still exists between the kind of support the pilot sites said they need and the kind of support they have been receiving from DHS across a range of issues, including the three focus areas of the project." [52] Moreover, they found in their "discussions at the pilot sites, that the quality of intelligence support in the wake of critical domestic and international homeland security-related incidents is a top priority for state and local fusion center leaders and a key determinant of how they evaluate DHS analytic support."[53]

The pilot project team focused on improving DHS response to SLFC requests for information (RFI), improving reporting and analysis that responds to SLFC mission-critical needs, and assisting the centers with their open source exploitation capabilities.[54] Upon completion of the pilot project in late 2007, the team reported enhancements that 'markedly improved DHS SLFC support efforts' at the pilot sites. They also reported that they had worked with I&A officers to

[48] 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*, Statement for the Record of Robert Riegle, Director DHS I&A SLPO, 111th Cong., 1st sess., April 1, 2009, p. 3. Hereafter: Riegle Statement, Apr. 1, 2009.

[49] 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.

[50] Between July and December 2008, a random selection of 12 fusion center directors from throughout the country were interviewed, as well as a major city police official and a state legislator who specializes in homeland security matters as part of his legislative portfolio. Hereafter: Comments to CRS by state and local officials, 2008.

[51] 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.

[52] Centra Technology, Inc., *Enhancing DHS Information Support to State and Local Fusion Centers: Results of the Chief Intelligence Officer's Pilot Project and Next Steps*, Feb. 20, 2008, p. 4. Hereafter: CINT Pilot Project Team Report.

[53] Ibid, p. 7.

[54] Ibid, p. 4.

develop a proposed action plan involving six core initiatives to implement these enhancements on a nationwide basis.[55]

One of pilot team's recommendations was to establish a staff element that will serve as focal point for all SLFC RFI's. The Director of the SLPO reported that in January 2008, I&A established a "Single Point of Service" program to give state and local customers "a 24-hour, one stop shopping resource to request support, communicate product requirements, and share critical information with DHS and its components." In the last quarter of 2008, that team serviced 659 support requests from 36 states.[56]

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."[57] 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.[58] 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.[59]

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

---

[55] Ibid.

[56] Riegle Statement, Apr. 1, 2009, p. 4.

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

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

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

[60] 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 Detail currently consists of four state and local law enforcement officers, a firefighter, and a part-time Tribal representative. In order to provide perspectives for IC reporting that goes beyond law enforcement, the Administration hopes to increase the membership to a total of ten state and local personnel, including a full-time tribal representative, a firefighter, a health and human services representative, a homeland security officer, and a state and local intelligence analyst.[61]

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. 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."[62]

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."[63] 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."[64]

Office of the Deputy Under Secretary for Mission Integration (DU/S-M)

This office is responsible for DHSI 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.[65] 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.[66]

[61] 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*, Statement for the Record of Michael E. Leiter, Director, NCTC, 110th Cong., 2nd sess., September 24, 2008.

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

[63] 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.

[64] Ibid, p. 4.

[65] 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.

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

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

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 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)[67] gives the HIST staff 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 the DU/S-I organization. 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,[68] of which 22% were border related.[69]

[67] 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

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

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

National Applications Office (NAO).

For more than 30 years, the Civil Applications Committee (CAC)[70] has facilitated requests by civil agencies to make use of space-based imaging and remote sensing capabilities for purposes such as monitoring volcanic activity, environmental and geological changes, hurricanes, and floods. 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.[71] I&A placed this office within the DU/S-M organization.

The establishment of this office, however, has been controversial.[72] 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, including all applicable privacy and civil liberties standards and that clear definitions of all proposed domains are established and auditable."[73] Congress also required the Government Accountability Office (GAO) to review the certification and report to Congress.[74]

Office of the Deputy Under Secretary for Field Operations (DU/S-F)

The DU/S-F manages the State and Local Program Office (SLPO). The SLPO is responsible for the DHS State and Local, Fusion Center Program which coordinates DHS support to state and local intelligence fusion centers and trains, equips, and deploys the department's cadre of field intelligence officers to those centers. [75]

State and Local Fusion Center (SLFC) Program

In an effort to strengthen intelligence and information sharing and analysis capabilities following the 9/11 attacks, states and major urban areas have established intelligence fusion centers.[76] 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

[70] For further information about the CAC, see the background paper published by the CAC Secretariat, July 2001. http://www.fas.org/irp/eprint/cac-fs.pdf

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

[72] 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, *Satellite Surveillance: Domestic Issues*, by Richard A. Best Jr. and Jennifer K. Elsea.

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

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

[75] DHS, *Interaction with State and Local Fusion Centers Concept of Operations*, December 2008, p. 12.

[76] 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.

criminal or terrorist activity; ... "[77] At the end of 2008, there were 72 centers operational within the United States and its territories covering 49 states, the District of Columbia (DC), and Guam. Fusion centers in Idaho, Puerto Rico, and the U.S. Virgin Islands are in the final stages of development.[78]

Congress mandated that DHS support fusion centers in the Implementing Recommendations of the 9/11 Commission Act of 2007.[79] 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.[80] Day-to-day program management of the Initiative is performed by the SLPO.

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 HIR's 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.

There are currently 34 officers deployed at 32 locations. DHS has also stated that they hope to deploy an officer to every fusion center in the country by the end of FY2010.[81] 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.[82]

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.[83] Its use of intelligence and infrastructure expertise to support risk management decision making is illustrated at **Figure 3**.

HITRAC is organized into two divisions responsible for the Center's principal functions.[84] The Risk Analysis Division performs infrastructure risk analysis and prioritization to support decision making. The division manages Congressionally-mandated and priority initiatives, including the

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

[78] National Criminal Intelligence Resource Center, Tallahassee, Florida, Dec. 17, 2008.

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

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

[81] "Riegle Statement, Apr. 1, 2009," p. 3.

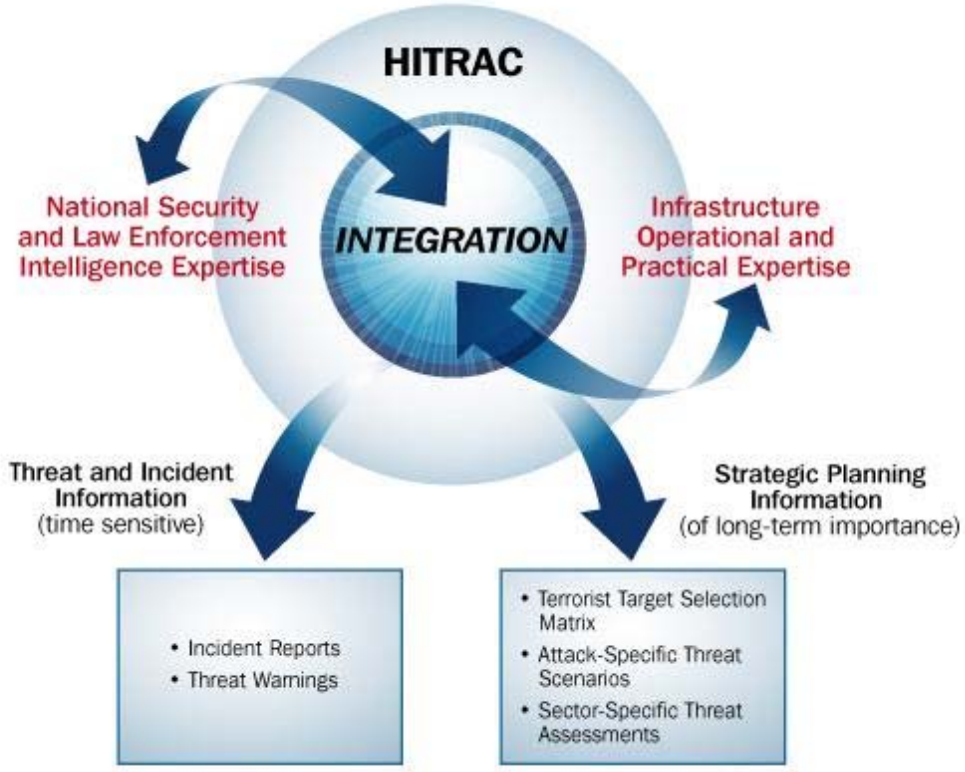
[82] "Comments to CRS by state and local officials, 2008."

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

[84] Ibid.

Tier 1 and Tier 2 Program[85] and the Critical Foreign Dependencies Initiative (CFDI).[86] 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).[87]

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



Source: DHS HITRAC, Dec. 29, 2008.

[85] 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

[86] 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

[87] 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 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. http://www.treas.gov/offices/international-affairs/cfius/

HITRAC products[88] 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 are intended to provide 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,[89] 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.[90] The execution of these authorities and responsibilities provides them with nominal operational independence. The Department has sought to develop an effective 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.[91] That role not only involves coordinating activities within DHS and its components, but also all

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

[89] 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.

[90] 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.

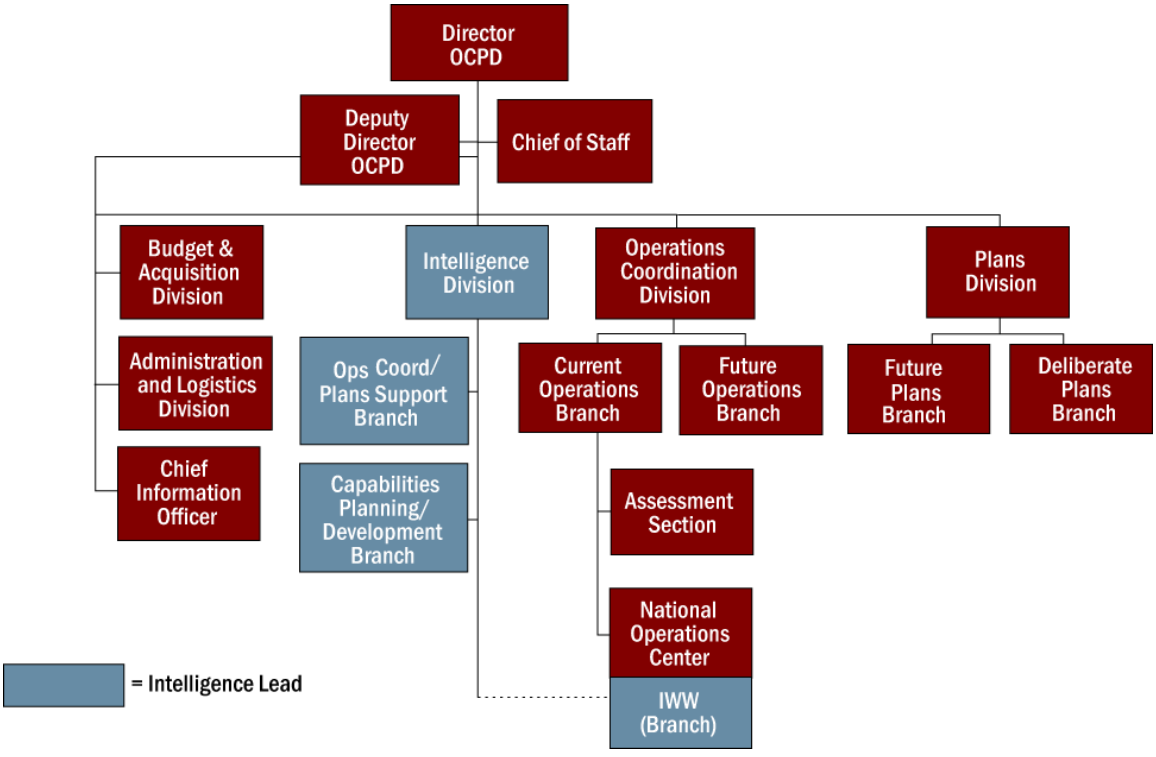
[91] According to Homeland Security Presidential Directive (HSPD)-5, *Management of Domestic Incidents*, February 28, 2003: "To prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive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

"Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies."[92]

The Intelligence Division at OPS is staffed by selected I&A personnel who are responsible to 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.[93] How the division is integrated into the OPS structure is shown in **Figure 4**.

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).

Figure 4. Directorate of Operations Coordination and Planning Organization



Source: DHS OPS, June 22, 2008.

[92] HSPD-5, paragraph 4.

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

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 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.[94]

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).[95] 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).[96] 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 works to implement 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

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

[95] 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.

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

(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.[97]

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.[98] The OIOC also functions as the situational awareness hub for CBP charged with 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 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.[99]

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)[100] 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.[101] All of this data is potentially useful to other Federal agencies with national security missions.

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

[98] Ibid.

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

[100] 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.

[101] 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://cbp.gov/xp/cgov/travel/admissability/authority_to_search.xml

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.[102] 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 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[103] 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.[104] A variety of data[105] 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.[106]

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

[102] In FY2008, at 327 ports of entry, CBP inspected over 396 million travelers; 122 million cars, trucks, buses, trains, vessels, and aircraft; and 25 million sea, truck, and rail containers. CBP also collected $32.5 billion in revenue, apprehended over 1 million aliens attempting to enter the United States illegally, and seized more than 2.78 million pounds of illegal narcotics. Source: CBP, *Securing America's Borders – CBP 2008 Fiscal Year in Review*, November 5, 2008. http://www.cbp.gov/xp/cgov/newsroom/highlights/08year_review.xml

[103] 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*.

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

[105] 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.

[106] 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," Aug. 11, 2008. http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/ace_factsheets/

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 information in ATS source databases against watch lists, criminal records, warrants, and patterns of suspicious activity identified through past investigations and intelligence. [107] ATS-P uses information from the following databases to assist in the development of the risk assessments discussed above:

- Advance Passenger Information System (APIS)[108]
- Non Immigrant Information System (NIIS)[109]
- Suspect and Violator Indices (SAVI)[110]
- Department of State visa databases[111]
- Passenger Name Record (PNR) systems[112]
- Treasury Enforcement Communications System (TECS)[113]
- Terrorist Screening Database[114]

[107] DHS Privacy Impact Assessment on ATS, p. 5.

[108] 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.

[109] 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

[110] 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.

[111] 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.

[112] 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.

[113] 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 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.

[114] 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, (continued...)

The results of queries in ATS-P are designed to signal to CBP officers that further inspection of a person may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise noted as a person of concern to law enforcement.

National Targeting Center (NTC)

The NTC utilizes the Automated Targeting System to support CBP officers at POE's. It is not an intelligence organization, but is a part of the CBP Office of Field Operations. 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 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.[115] 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.[116] 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.[117] 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

(...continued)

September 2007, p. i, http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf.

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

[116] 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.

[117] 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).

criteria.[118] 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.[119] 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.[120] In late 2007, targeting and analysis within NTCC led to the intercept and seizure of over $3 million worth of assault rifles and small arms destined for Central America.[121]

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.[122]

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[123] co-produced by CBP and the NCTC. The report, which surveyed the arrest records of "special interest aliens"

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

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

[120] Ibid.

[121] Ibid.

[122] 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.

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

(SIA)[124] 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.[125] In October 2007, the organization was fully integrated into the CBP OIOC and its name changed to the Border Field Intelligence Center.

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)[126] 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[127] across the nation's borders and

[124] 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.

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

[126] 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

[127] 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.

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.[128]

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.[129] 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 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).[130]

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.[131] For example, if an increase in aliens entering the United States illegally from or through a particular country were

[128] 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.

[129] 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.
http://www.ofcm.gov/mpar-symposium/presentations.htm

[130] 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.

[131] 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).

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.[132]

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 protect the American people from the illegal introduction of goods and the entry of terrorists and other criminals seeking to cross our Nation's borders and to protect U.S. Government facilities and occupants.[133] ICE investigates violations of U.S. customs and immigration laws by targeting the people, money, and materials that support terrorism and other criminal activities that pose a threat to national security. It has five operational divisions:

- Office of Investigations (OI). OI is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States.[134] Of note, ICE Special Agents are the largest non-FBI component of the Joint Terrorism Task Forces (JTTF). [135]
- 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.[136]
- Federal Protective Service (FPS). The FPS is responsible for policing, securing, and ensuring a safe environment in which federal agencies can conduct their business.[137]

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

[133] ICE, *FY2009 Fact Sheet*, Oct. 28, 2008. http://www.ice.gov/pi/news/factsheets/

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

[135] 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/

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

[137] ICE, *FPS Factsheet*, Nov 20, 2008. http://www.ice.gov/doclib/pi/news/factsheets/federal_protective_service.pdf

- Office of International Affairs (OIA). With 54 offices abroad, OIA develops partnerships with foreign governments to advance the homeland security mission.[138]
- 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.[139]

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 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.

The Office of Intelligence is led by a Director and consists of four divisions and 26 Field Intelligence Groups.[140] 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.

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. Another unit, the Tactical Intelligence Center located in Bay Saint Louis, Mississippi, works with the National Security Agency and the HSPSU to integrate and analyze signals intelligence, human intelligence, and law enforcement information to identify new human smuggling targets for ICE investigations, assist NSA in SIGINT targeting, and support the HSPSU in performing strategic level intelligence analysis.

[138] ICE, *ICE Offices*. http://www.ice.gov/about/operations.htm

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

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

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 Intelligence Watch and two other programs of note:

- 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.
- Operation Last Call. This is a nationwide effort to collect, analyze, and disseminate intelligence derived from the thousands of individuals who enter the ICE detention and removal system each year. Special emphasis is placed on the cultivation of sources with knowledge of or access to information relating to threats against the homeland, human smuggling and trafficking, contraband smuggling, terrorist or other criminal organizations, and other activities of operational interest to ICE or the IC.

The Intelligence Systems and Security Division has oversight over the information technology systems to include all classified and unclassified applications, systems, and networks of the Office of Intelligence.

Field Intelligence Groups (FIG)

The Office of Intelligence field organization consists of 26 FIG's that are aligned and co-located with ICE SAIC offices throughout the United States. They replaced the former Field Intelligence Units in a recent reorganization of the ICE field intelligence structure intended to improve connectivity and working relationships with ICE operational elements as well as enhance coordination with other Federal, state, local, and cross border partners. [141]

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.

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

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

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

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

Border-Related Enforcement Operations Supported by the BVIC

ICE is engaged in several operational initiatives. The following three have a border focus and are supported by the BVIC.

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 12 BEST task forces, eight on the southwest border, two on the northern border and two at major seaports (Los Angeles and Miami). 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.

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

Armas Cruzadas

Armas Cruzadas is a partnership between U.S. and Mexican law enforcement agencies. [144] 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.[145]

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 illicit funds between banks and other financial institutions more difficult, criminal organizations are increasing their use of bulk cash smuggling.[146] 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. [147]

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.

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

[145] 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.

[146] 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.

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

Congress formally established the HSTC in the Intelligence Reform Act and Terrorism Prevention Act of 2004.[148] 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[149] 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."[150] 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 review legislatively-mandating minimum staffing by agencies critical to the Center's success. At present, each participating agency provides staff "out of hide," meaning they are not reimbursed for the personnel they detail to HSTC. To alleviate this impact, Congress may also consider dedicated funding for the detailee positions at the Center.

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

[149] 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/

[150] 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.

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.[151] 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.[152] The three principal immigrant service activities of USCIS are the adjudication of immigration petitions; the adjudication of naturalization petitions for lawful permanent residents to become U.S. citizens; and the consideration of refugee and asylum claims, and related humanitarian and international concerns.[153]

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.[154] Thus its activities are limited to adjudication of immigration benefits, which includes conducting background checks on applications and petitions. 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 7,000 Permanent Resident Cards (Green Cards), adjudicates 200 refugee applications, and naturalizes 3,000 new civilian citizens and 27 new citizens who are member of the U.S. Armed Forces.[155]

USCIS also has the authority to detect and combat immigration fraud.[156] Individuals and organizations intent on harming the United States have become increasingly sophisticated in their methods of gaining entry into the country.[157] 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. [158]

---

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

[152] 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

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

[154] In the FY09 appropriations bill (P.L. 110-329, Sep. 30, 2008), USCIS received $102 million in direct appropriations versus $2,539 million in gross budget authority through revenues from collected fees. See CRS Report RL34482, *Homeland Security Department: FY2009 Appropriations*, by Jennifer E. Lake et al., p. 93.

[155] USCIS FY2007 Annual Report, p. 11.

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

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

[158] 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

In 2003, USCIS established the Office of Fraud Detection and National Security (FDNS). This office is part of the USCIS Directorate of National Security and Records Verification. It consists of four branches that 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; performing as USCIS' primary conduit to and from law enforcement and intelligence agencies. [159]

The USCIS Intelligence Branch

Within FDNS, there is an Intelligence Branch that analyzes, produces, and disseminates all-source intelligence and immigration information to support the USCIS fraud detection and national security missions. The branch directs and manages assets and resources at headquarters and at five USCIS Service Centers to detect emerging fraud trends and indicators, and to deter immigration fraud with a nexus to national security. It also is a conduit for sharing, coordination, and collaboration of intelligence information with the IC and various law enforcement agencies. To this end, they have placed liaison officers within I&A, the National Operations Center, the Terrorist Screening Center, NCTC, and as the DHS detailee to INTERPOL headquarters in Lyon, France.

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 and headquarters leadership at USCIS, DHS components, and other Federal, state, and local agencies.[160] 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)[161] 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.[162] 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 its 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 open investigation by Federal law enforcement.

[159] USCIS briefing to CIS, July 8, 2008.

[160] Ibid.

[161] 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.

[162] 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

Transportation Security Administration (TSA) Intelligence Element

In November 2001, Congress established TSA through the *Aviation and Transportation Security Act of 2001 (ATSA)*.[163] 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.[164] 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 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."[165] 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.[166] 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.

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

[164] 49 U.S.C. 114.(d).

[165] 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.

[166] 49 U.S.C. 114(f).

TSA-OI Analysis

TSA 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. TSA-OI also reviews and analyzes the suspicious activity reporting by Transportation Security Officers, Behavior Detection Officers, and FAMS. TSA-OI 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 TSA OI's relationship with its stakeholders. TSA-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)[167] for transportation security. TSA-OI is in the process of developing both the concept 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.

TSA 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 Transportation 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 TSA 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.

TSA-OI analytic products include the Administrator's Daily Intelligence Brief, Information Bulletins and Circulars, the Weekly Report of Suspicious Incident Reports (SIR), and the Transportation Intelligence Gazette (TIG). The SIR and the TIG 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.

[167]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

Field Intelligence Officer Program

TSA-OI has deployed field intelligence officers to major airports throughout the United States. They work directly for TSA 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.[168] 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."[169] He goes on to say "[a]s important as it is to detect threat objects, it is imperative that we use intelligence to aid in the identification and interception of the people who would do us harm."[170]

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

No Fly and Selectee Lists

In addition to attempting to uncover 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."[171]

---

[168] 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.)

[169] 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.

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

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

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)…"[172] 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.[173] 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.[174] 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.[175] It was even reported last year that some Federal Air Marshals were denied boarding on flights they were assigned to protect because their names matched those on the No Fly list.[176]

The U.S. Government, however, 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.[177] 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).[178]

---

[172] Ibid, p. 3.

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

[174] 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

[175] 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

[176] 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/

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

[178] 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. Some have questioned the program's effectiveness. At a September 2008 hearing, Representative Sheila Jackson Lee stated that "individuals who have gone through the redress process continue to experience problems when traveling." See 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*, Opening Statement of Representative Sheila Jackson Lee, 110th Cong., 2nd sess., Sep. 9, 2008.

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. TSA-OI, however, plays a limited role in who is added to these lists. According to former Assistant Administrator Bill Gaches, the preponderance of the No Fly and Selectee individuals are nominated for inclusion on these lists by other core intelligence and law enforcement agencies.[179]

Computer Assisted Passenger Prescreening System (CAPPS)[180]

CAPPS was originally developed in the 1990's by the Federal Aviation Administration (FAA) for secondary screening based on certain travel behaviors reflected in their reservation information that are associated with threats to aviation, as well as a random selection of passengers. As implemented prior to 9/11, CAPPS flagged passengers with a score above a certain threshold for additional screening, but only of their checked baggage since explosives in checked baggage were believed to be the primary threat at the time.

After 9/11, the CAPPS criteria were adjusted to mitigate terrorists risks against aviation including hijackings. At present, air carriers are responsible for matching passenger names against the greatly expanded No Fly and Selectee lists provided to them by TSA. Passengers designated as "selectees" today by CAPPS are subject to a pat down search and additional screening of their checked and carry-on baggage.

TSA-OI is responsible for the intelligence analysis underpinning the risk factors and the relative weights assigned to these factors. TSA declines to publish the factors, but there has been much speculation in the media about them. In 2004, a TSA official speaking to the Associated Press on condition of anonymity indicated that travelers may become selectees because of "paying in cash or frequently buying one-way tickets."[181] A TSA spokesman has stated that some passengers are also selected at random.[182]

Secure Flight

After abandoning an effort to establish a follow-on system to CAPPS I (called CAPPS II), 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.[183] 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

[179] 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.

[180] This system is commonly referred to as CAPPS I. Development of a follow on system, CAPPS II, was discontinued by TSA in 2005. In its place, TSA has proposed *Secure Flight.*

[181] Associated Press, "Women Complain About Airport Patdowns," Nov. 30, 2004.

[182] Ibid.

[183] 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

watchlists with non-threatening passengers whose names are similar.[184] 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."[185]

On March 31, 2009, TSA announced that it has begun implementation of Secure Flight by assuming watch list matching responsibility for passengers on domestic commercial flights with four volunteer aircraft operators and will add more carriers in the coming months. TSA's goal is to vet 100 percent of all domestic commercial flights by early 2010 and 100 percent of all international commercials flights (a function now performed by CBP) by the end of 2010.[186]

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.[187]

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 stated 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-board, armed federal air marshals."[188] 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

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

[185] Ibid.

[186] TSA Press Release, "TSA's Secure Flight Begins Vetting Passengers, Mar. 31, 2009. http://www.tsa.gov/press/releases/2009/0331.shtm

[187] 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

[188] 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

marshals being on flights they may be interested in taking over or otherwise disrupting."[189] However, TSA has publicly stated that the number is in "the thousands."[190]

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. TSA-OI provides intelligence to support FAMS mission planning. TSA-OI has an intelligence unit, manned 24/7, at the TSOC.

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

As a nation of travelers and traders, America has a strategic interest in the maritime domain.[191] 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.[192] 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.[193]

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.[194] 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.[195] In March 2003, pursuant to the Homeland Security Act, the USCG was transferred from the Department of Transportation to DHS.[196]

The USCG has several diverse missions—national defense, homeland security, maritime safety, and environmental and natural resources stewardship.[197] To accomplish these missions, the USCG

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

[190] Ibid.

[191] 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.

[192] 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 2006, there were 9 million cruise line passenger embarkations. Direct spending by cruise lines and their passengers totaled $17.6 billion. Source: Business Research and Economic Advisors, *The Contribution of the North American Cruise Industry to the U.S. Economy in 2006*, Aug. 2007, p. 6. http://www.cruising.org/press/research/U.S.CLIA.Economic.Study.2006.pdf

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

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

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

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

[197] There are eleven statutorily-mandated USCG mission programs: [197] 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.

has authorities unique within the Federal government. It is both an armed service[198] and the nation's primary maritime law enforcement agency.[199]

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.[200] 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 States."[201] Since it grants time and distance to detect, deter, interdict, and defeat adversaries,[202] maritime domain awareness has been enshrined as a principal objective of the *National Strategy for Maritime Security*.[203]

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[204]—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:[205]

- 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

[198] 14 U.S.C. §1.

[199] 14 U.S.C. §2.

[200] 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

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

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

[203] The White House, *National Strategy for Maritime Security Maritime Security*, Sep. 2005. http://www.whitehouse.gov/homeland/4844-nsms.pdf

[204] 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.

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

December 2001 when Congress amended the *National Security Act of 1947*.[206] 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 matters to the Commandant of the Coast Guard, and is the Senior Official of the Intelligence Community for the Coast Guard National Intelligence Element.[207] 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.[208] 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)[209] on adversary disposition, plans, and intent to facilitate tactical, operational, and strategic maritime domain dominance."[210]

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

[206] 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.

[207] 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.

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

[209] 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.

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

capability will be installed on the new National Security Cutter[211] 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.[212] The USCG sees this capability as the cornerstone of the Global Maritime Intelligence Integration effort.[213]

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 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 CGIS conducts criminal and personnel security investigations within the Coast Guard's area of responsibility. As a federal law enforcement agency whose authority is derived from 14 U.S.C. §95, USCG special agents conduct investigations of actual, alleged, or suspected criminal activity; carry firearms; execute and serve warrants; and make arrests.[214]

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.[215] 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

[211] 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.

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

[213] 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.

[214] USCG, Briefing on CGIS to CRS, Oct. 27, 2008.

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

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:[216]

- 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.

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, people and cargo. 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.[217] 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.[218]

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

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

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

Area and District Intelligence Staffs

These staffs provide intelligence support to their respective commanders and the International Ship and Port Facility Code (ISPS) Program.[219] District intelligence staffs are also responsible for coordinating human intelligence (HUMINT) collection, conducting regional law enforcement and intelligence liaison, and managing the Sector Intelligence Officers and Field Intelligence Support Teams.[220]

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 conduct liaison with Federal, state, local, tribal, and industry partners.[221]

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. In addition, the SIS' assist counterintelligence efforts by reporting on foreign vessels that are collecting intelligence against the United States in or near domestic ports.[222]

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

Although the USSS[223] 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.[224]

[219] 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).

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

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

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

[223] 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.

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

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.[225]

USSS Organizational Structure

The USSS employs approximately 3,200 special agents, 1,300 Uniformed Division officers, and more than 2,000 other technical, professional, and administrative support personnel. They work at the headquarters in Washington, D.C. and in 139 field offices and units within the United States and its territories and 22 offices in 18 foreign countries.[226] 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.

- Investigations. This office investigates counterfeiting and other crimes against the integrity of the nation's financial infrastructure and payment systems.[227]
- 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.[228] 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 Security Special Events (NSSE).[229]

[225] 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

[226] USSS Briefing for CRS, Oct. 8, 2008.

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

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

[229] 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 (continued...)

- 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 efforts to: (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.[230] 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.[231]

National Threat Assessment Center (NTAC)[232]

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.[233]

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

(...continued)

RS22754, *National Special Security Events*, by Shawn Reese.

[230] The White House, ExpectMore.gov, "Secret Service: Protective Intelligence Assessment," 2007. http://www.whitehouse.gov/omb/expectmore/detail/10002412.2004.html

[231] Ibid.

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

[233] 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).

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.[234]

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.[235]
- 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.[236]
- 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 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,[237] 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 DHSI. Former Under Secretary Allen saw the Department itself—both headquarters and operational components—as I&A's primary customer. He stated that:

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

[235] 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).

[236] 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).

[237] 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

> "... 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."[238]

But, as has been noted, DHSI also has responsibilities to support the Secretary and 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 approaches the Congress may decide to consider in exercising its oversight responsibility.

Support to State and Local Fusion Centers

Institutionalizing the State and Local Fusion Center (SLFC) Pilot Project Recommendations

Over one year has passed since the SLFC Pilot Project Team reported that its initiative at six pilot fusion centers led to improvements in the DHS response to SLFC requests for information, reporting and analysis that responds to SLFC mission-critical needs, and assistance to centers with their open source exploitation capabilities.[239] In its 2008 report to the Under Secretary for I&A, the pilot team reported that they had worked with I&A officers to develop a proposed action plan involving the following six core initiatives to implement these enhancements on a nationwide basis:[240]

- Establish a staff element that will serve as focal point for all SLFC requests for information (RFI) expanding on the RFI process established for the six pilot sites.
- Establish a DHS production planning process that is focused on identified SLFC needs.
- Establish the I&A Collections Requirements Division as the focal point for an integrated DHS program to assist the SLFC's to develop their Open Source exploitation capabilities.
- Strengthen DHS leadership direction of the SLFC support effort and integrate administrative and logistical support with the substantive support provided by the analytical divisions in I&A.

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

[239] "CINT Pilot Project Team Report," p. 4.

[240] Ibid.

- Develop performance metrics and collect customer feedback in order to assist the SLFC Support Leadership Council and I&A Divisions evaluate the quality of SLFC support.
- Develop a long-term strategic plan for integrating all DHS components as well as key IC agencies into an I&A-led SLFC intelligence support activity.

Institutionalizing those improvements within I&A and throughout the entire national SLFC network of 72 centers may prove to be a big challenge. Congress may choose to examine I&A's implementation of the pilot project team's recommendations and the effect these have had on the focus and relevance of I&A's products for state, local, and tribal customers.

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.[241] The fusion center program and the Nationwide Suspicious Activity Report Initiative (NSI)[242] 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 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 would necessarily have to acquire a 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.[243]

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

[242] The 2007 *National Strategy for Information Sharing* called for the Federal Government to support the development of a nationwide SAR process that protects the civil liberties of Americans. The NSI is an outgrowth of a number of separate but related activities over the last several years that responds directly to the Strategy's mandate, with the long term goal of having most Federal, state, local, and tribal law enforcement organizations participating in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially terrorism-related." See DNI, Program Manager for ISE, *ISE SAR Functional Standard Suspicious Activity Reporting, Version1*. http://www.ise.gov/docs/ctiss/ISE-FS-200SARFunctionalStandardIssuanceVersion1.0.pdf

[243] 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

An evaluation is currently underway with three state and nine urban fusion centers to work out ways to harmonize varying state privacy protocols and communications. Congress may be asked to consider providing funding and leadership to expand this infrastructure capability to all of the current 72 fusion centers.

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.[244] 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).[245] 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 opt 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.

Quadrennial Homeland Security Review (QHSR)

Former Secretary Chertoff has said that "DHS must base its work on priorities that are driven by risk."[246] 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).[247] DHSI identifies, measures, and monitors the threat variable in the DHS risk equation.

The role of DHSI in risk management decision making at the Department is another area Congress may explore. A recent study by the Homeland Security Institute noted that DHS risk assessments require threat inputs but generating useful threat judgments is challenging.[248] It suggested ways to improve risk and intelligence analyst collaboration to better support DHS decision making.

Later this year, Congress will have 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 Department is to conduct its first comprehensive

[244] 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.

[245] 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.

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

[247] DHS, *FY2008 Homeland Security Grant Program: Program Guidance and Application Kit*, February 2008, pp. 2-3.

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

examination of homeland security called the QHSR,[249] which will include recommendations regarding the long-term strategy and priorities for homeland security and guidance on the Department's programs, assets, capabilities, budget, policies, and authorities.

On December 31, 2009, the Department is required to submit to Congress a report covering:

- The results of the QHSR.
- A description of the threats to the nation's security interests.
- The updated national homeland security strategy, including a prioritized list of the critical homeland security missions of the nation.
- A description of the interagency cooperation, preparedness of federal response assets, infrastructure, and budget plan.
- The status of cooperation among federal agencies and between the federal government and state, local, and tribal governments.

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."[250]

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 was understandably devoted to aviation security—an amount proportionally larger than that of other transportation modes or critical infrastructure. Since 9/11, al-Qa'ida and other terrorist groups with anti-Western and anti-American ideologies have committed several deadly terrorist attacks including:

- 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

[249] 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.

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

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.

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."[251]

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.[252]

Pyroterrorism is just one example of many alternative hypotheses that homeland security risk managers may consider in order to avoid what was famously described in the *9/11 Commission Report* as "a failure of imagination."[253] 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 choose to explore:

- How I&A will support the Department's 2009 QHSR effort.
- 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.

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

[252] Ibid, p. 17.

[253] *9/11 Commission Report*, p. 339.

Author Contact Information

Mark A. Randol
Specialist in Domestic Intelligence and Counter-Terrorism
mrandol@crs.loc.gov, 7-2393