Federal Law Enforcement Intelligence

11

CHAPTER ELEVEN

Federal Law Enforcement Intelligence

Many federal agencies have reengineered their intelligence function since 9/11. Intelligence products have been redesigned or new products developed, dissemination methods have been revised, greater attention has been given to providing critical information that is unclassified for wide consumption by state, local, and tribal law enforcement (SLTLE), and new offices and initiatives have been developed. More information is being produced and disseminated more widely than in the history of law enforcement. Among the challenges that law enforcement now faces is accessing that needed information and using it with efficacy.

In many instances, federal intelligence initiatives are still in a dynamic state and, as a result, it is virtually impossible to provide an exhaustive discussion of them all. This chapter, therefore, will identify those federal intelligence resources of greatest use to SLTLE, their intelligence products, and the agencies' contact or access information. In addition, the chapter will present a broader discussion of the FBI than of other agencies because of the significant changes that have occurred in the FBI's structure and processes and the importance of the SLTLE/FBI relationship in counterterrorism and control of criminal enterprises.

While federal agencies have attempted to provide more unclassified information to America's law enforcement agencies, a significant amount of classified information remains relating to criminal investigations and terrorism. The FBI, therefore, has made a commitment to increase security clearances for SLTLE officers. Despite this, controversies and questions remain. As a result, dealing with the issue of classified information seems to be the first place to start when discussing intelligence from federal agencies.

181 http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html which amends a previous Executive Order on classified information.

Classified Information

There is often a mystique about classified information, leading most people after seeing a collection of classified documents to ask, “That's it?” For the most part, the key distinction between classified and unclassified information is that the former contains “sources and methods.”

Some definitions: According to Executive Order 12958[181] issued on March 23, 2003, information at the federal level may be classified at one of three levels:

- “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

- "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

When an intelligence analyst from the FBI, Drug Enforcement Administration (DEA), or other federal agency receives raw information, he or she must assess it for its source reliability and content validity. The "weight" of each of these variables and their corollaries provide significant insight into the credibility and importance of the information received. The higher the credibility and the greater the corroboration, the higher the "accuracy" of the information. Collectively, as credibility increases, the greater the need for a policy response.

For example, let us say that the FBI receives information about a possible terrorist attack. If the reliability and validity are very low, little credibility will be placed in the threat, although the FBI will develop corroboration and perhaps plan for a response. As validity and reliability increase, the greater credibility will result in devoting more resources to corroboration and a response. If validity and reliability are high, particularly if corroborated, the FBI will initiate a policy response. Policy responses may include proactive investigations, target hardening, and in the most severe cases, the Department of Homeland Security (DHS) may increase the threat level of the Homeland Security Advisory System (HSAS), triggering a significant string of policy responses at all levels of government. This admittedly oversimplified illustration demonstrates the need for analysts to know the sources and methods of information so that they can make the best judgments in their analysis.

Beyond analysts, it is important for investigators, too, to know sources and methods to work their leads. Members of the Joint Terrorism Task Forces (JTTF) need security clearances to conduct their investigations effectively. Do other members of SLTLE agencies need to have security clearances? Certainly not, but who receives a clearance depends on a number of factors. As a rule, SLTLE executives may apply for a clearance for three reasons:

1. To understand the complete nature of a threat within their jurisdiction.
2. To make management decisions, ranging from the assignment of personnel to investigations to the need for extending shifts and canceling officers' leaves should the threat condition warrant it.
3. As a courtesy to the executive who is contributing staff and resources to counterterrorism. This courtesy is not superficial, but aids the executive on matters of accountability.

For other members of an SLTLE agency, decisions should be made on a case-by-case basis to determine if the security clearance best serves the community's and, hence, national, interests. There are three reasons for not having an "open application" for security clearances. First, security clearance means having access to classified information. Before authorizing the application for a clearance, the agency should assess the applicant's "right to know" and "need to know" classified information should be considered. It may be reasonable to grant a security clearance to a local police detective who works organized crime cases; however, a traffic commander would have virtually no need for a clearance.

Second, the clearance process is labor intensive and expensive. It is simply not prudent fiscal management to authorize clearance investigations in all cases. Third, conducting an excess number of clearance investigations slows the process, thereby taking longer to process clearances for those persons who may be in more critical positions.

In most cases, the FBI will begin consideration of a clearance investigation for an SLTLE officer by examining local issues on a case-by-case basis.[182] For those who seek to apply for a security clearance, the appropriate forms and fingerprint cards can be obtained from the local FBI Field Office. Appendix E describes the process for gaining a clearance and provides a list of frequently asked questions and their answers.[183]

Sensitive But Unclassified (SBU) Information[184]

Since it is not feasible for every law enforcement officer to have a security clearance, there is a mechanism to get critical information into the hands

182 The FBI provides the following guidance: Most information needed by state or local law enforcement can be shared at an unclassified level. In those instances where it is necessary to share classified information, it can usually be accomplished at the Secret level. Local FBI Field Offices can help determine whether or not a security clearance is needed, and if so, what level is appropriate.

183 The National Security Clearance Application (Standard Form SF-86) can be downloaded from http://www.usaid.gov/procurement_bus_opp/procurement/forms/SF-86/sf-86.pdf.

184 As a means to aid in clarity, the FBI is moving away from the SBU label and using/will use Law Enforcement Sensitive in all cases, rather than using both labels.

of officers while not jeopardizing classified information: Declassifying the reports by removing sources and methods and labeling the report as SBU achieves this goal. This process is accomplished in two ways. One way is to use a "tear line" report in which an intelligence report has a segment,

> Intelligence products have been redesigned or new products developed, DISSEMINATION methods have been revised, greater attention has been given to providing CRITICAL INFORMATION that is unclassified for wide consumption by SLTLE…

perhaps at the bottom of the page, where critical information is summarized and sources and methods are excluded. This portion of the report may be "torn off" (at least figuratively) and shared with persons who have a need to know the information but do not have a security clearance. The second method is to write intelligence products in a way that relays all critical information but excludes data that should remain classified. (The FBI Office of Intelligence is working specifically on this process.) Following this process, SLTLE officers receive documents that are labeled "Sensitive But Classified" or "Law Enforcement Sensitive", thereby raising the question, "What does this mean?"

Over time some agencies have established procedures to identify and safeguard SBU information. Generally, this unclassified information is withheld from the public for a variety of reasons, but has to be accessible to law enforcement, private security, or other persons who have a responsibility to safeguard the public. The term SBU has been defined in various presidential-level directives and agency guidelines, but only indirectly in statute. Agencies have discretion to define SBU in ways that serve their particular needs to safeguard information. There is no uniformity in implementing rules throughout the federal government on the use of SBU.[185] There have been even fewer efforts to define and safeguard the information at the state, local, and tribal levels. There is an intuitive

185 For a detailed review of the SBU meaning and how it is defined and used by different statutes and regulations, see: Knezo, Genevieve J. *Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information*. Washington, DC: Congressional Research Service.

understanding, but no formal process to control the information. Perhaps some guidance is being provided by the DHS which issued a directive in 2004 on "For Official Use Only" (FOUO) information.

DHS "For Official Use Only" (FOUO) Information

The FOUO label is used within DHS "…to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of a federal program, or other programs or operations essential to the national interest."[186] FOUO is not classified information, but information that should be distributed only to persons who need to know the information to be aware of conditions that will help keep the homeland and, hence, the community, secure. Within DHS, the caveat "For Official Use Only" will be used to identify SBU information within the DHS community that is not otherwise governed by statue or regulation. At this point the designation applies only to DHS advisories and bulletins.

Since SLTLE agencies will encounter these labels when receiving federal intelligence products it is useful to know the framework from which they arise. At a practical level, the rule of thumb for law enforcement officers is to use good judgment when handling such materials. This does not mean that SLTLE officers may not disseminate this information further unless prohibited from doing so as indicated on the report. Rather, the officer should use the information in a manner that meets community safety needs, including disseminating portions of the information to those segments of the community that would benefit from the data contained in the report.

FEDERAL INTELLIGENCE PRODUCTS[187]

In light of the perspective regarding classification of federal intelligence reports, the following discussions will describe federal intelligence products, virtually all of which will be SBU.

186 Department of Homeland Security, Management Directive System, MD Number: 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. May 11, 2004.

187 Information in this section is based on interviews with FBI Office of Intelligence personnel, reviews of the Office of Intelligence Concepts of Operations (ConOps) and Congressional testimony of Director Mueller. See http://www.fbi.gov/congress/congress04/mueller022404.htm.

FBI Office of Intelligence

The FBI created the Office of Intelligence (OI) to establish and execute standards for recruiting, hiring, training, and developing the intelligence analytic work force, and ensuring that analysts are assigned to operational and field divisions in line with intelligence priorities. The FBI also established a new position, the executive assistant director for intelligence, who joins the three other executive assistant directors in the top tier of FBI management.[188] However, it is important to recognize that the OI goes far beyond being an analyst work force. Rather, it serves to provide centralized management of the FBI's intelligence capabilities and functions in the form of policy, standards, and oversight. Moreover, it embodies the Intelligence-Led Policing philosophy by serving as the driving force to guide operational activities.

To maximize the effectiveness of the intelligence process, the FBI's Office of Intelligence established a formal "intelligence requirements" process for identifying and resolving intelligence information (or information) needs. This is intended to identify key gaps–unanswered questions about a threat – in the FBI's collection capability that must be filled through targeted collection strategies.

188 For more information on the FBI Office of Intelligence, see http://www.fbi.gov/intelligence/intell.htm.

In order to maximize the effectiveness of the intelligence process, the FBI OI has established a formal "INTELLIGENCE REQUIREMENTS" process for IDENTIFYING intelligence information (or information) needs and resolving them.

As a means to ensure that FBI-wide collection plans and directives are incorporated into field activities, every FBI Field Office has established a Field Intelligence Group (FIG). The FIG is the centralized intelligence component in each field office that is responsible for the management, execution, and coordination of intelligence functions. FIG personnel gather, analyze, and disseminate the intelligence collected in their field

offices. Staffed by both special agents and intelligence analysts, the FIG serves as the primary intelligence contact point for SLTLE agencies.

Field offices are also supporting the "24-hour intelligence cycle" of the FBI by using all appropriate resources to monitor, collect, and disseminate threat information, investigative developments (e.g., urgent reports), and other significant raw intelligence to meet the executive information needs of the field offices, other field offices, FBI Headquarters, Legal Attachés, and other federal or state and local agencies.

The reengineered FBI Office of Intelligence has developed two threat-based joint intelligence products and a third product known as the Intelligence Information Report. All of these products may be accessed by law enforcement at all levels of government.

- ***Intelligence Assessment:*** A comprehensive report on an intelligence issue related to criminal or national security threats within the service territory of an FBI Field Office. The assessment may be classified at any level or be unclassified depending on the nature of the information contained in the report. In most cases when the report is unclassified, it is Law Enforcement Sensitive.
- ***Intelligence Bulletin:*** A finished intelligence product in article format that describes new developments and evolving trends. The bulletins typically are SBU and available for distribution to state, local, and tribal law enforcement.
- ***Intelligence Information Report:*** Raw, unevaluated intelligence concerning "perishable" or time-limited information about criminal or national security issues. While the full IIR may be classified, state, local, and tribal law enforcement agencies will have access to SBU information in the report under the tear line.

An immediate source for FBI intelligence products is the Field Intelligence Group (FIG).[189] In addition, SLTLE agencies are able to gain direct access to these reports by secure email through Law Enforcement Online (LEO), the National Law Enforcement Telecommunications System (NLETS), or the Joint Regional Information Exchange System (JREIS). When circumstances warrant, the FBI and DHS will produce an intelligence product jointly and disseminate it to the appropriate agencies.

189 The FIG should be contacted at your local FBI Field Office. Contact information for all field offices is at http://www.fbi.gov/contact/fo/fo.htm

FBI Counterterrorism[190]

Designated as the top priority for the FBI, countering terrorists' threats and acts is a responsibility requiring the integration of effective intelligence and operational capabilities. In support of the different intelligence units and activities discussed previously, the FBI has developed or enhanced a number of initiatives that seek to fulfill its counterterrorism mandate. While these are largely not intelligence programs per se, they all contribute to the intelligence cycle and consume intelligence for prevention and apprehension. A brief description of these initiatives will provide a more holistic vision of the FBI's counterterrorism strategy.

Specialized Counterterrorism Units

To improve its system for threat warnings, the FBI established a number of specialized counterterrorism units. They include the following:

- CT Watch, a 24-hour Counterterrorism Watch Center that serves as the FBI's focal point for all incoming terrorist threats
- The Communications Analysis Section analyzes terrorist electronic and telephone communications and identifies terrorist associations and networks
- The Document Exploitation Unit identifies and disseminates intelligence gleaned from million of pages of documents or computers seized overseas by intelligence agencies
- The Special Technologies and Applications Section provides technical support for FBI Field Office investigations requiring specialized computer technology expertise and support
- The interagency Terrorist Financing Operations Section is devoted entirely to the financial aspects of terrorism investigations and liaison with the financial services industry.

Intelligence gleaned from these special information and analysis resources is placed in the appropriate format (i.e., Bulletins, Assessments, IIR, advisories) and distributed to the field through appropriate dissemination avenues.

190 Contact for the various counterterrorism program resources should be coordinated through your local FBI JTTF or FIG. The FBI Counterterrorism Division's comprehensive web page http://www.fbi.gov/terrorinfo/counterrorism/waronterrorhome.htm.

FBI Information Sharing and Operational Coordination Initiatives

To defeat terrorists and their supporters, a wide range of organizations must work together. The FBI, therefore, has developed or refined both operational and support entities intended to bring the highest possible level of cooperation with SLTLE agencies, the Intelligence Community, and other federal government agencies.

- Joint Terrorism Task Forces (JTTF). Cooperation has been enhanced with federal, state, local, and tribal law enforcement agencies by significantly expanding the number of JTTFs. The task forces, which are operational in nature, tackle a wide array of potential terrorist threats and conduct investigations related to terrorist activities within the geographic region where the particular JTTF is headquartered.
- The National JTTF (NJTTF). In July 2002, the FBI established the NJTTF at FBI Headquarters and staffed it with representatives from 30 federal, state, and local agencies. The NJTTF acts as a "point of fusion" for terrorism information by coordinating the flow of information between Headquarters and the other JTTFs located across the country and between the agencies represented on the NJTTF and other government agencies.
- The Office of Law Enforcement Coordination (OLEC). The OLEC was created to enhance the ability of the FBI to forge cooperation and substantive relationships with all SLTLE counterparts. The OLEC, which is managed by FBI Assistant Director Louis Quijas, a former chief of police, also has liaison responsibilities with the DHS, COPS Office, Office of Justice Programs, and other federal agencies.

Terrorist Threat Integration Center (TTIC)[191]

The mission of TTIC is to enable full integration of terrorist threat-related information and analysis derived from all information and intelligence sources in the law enforcement and intelligence communities. The center is an interagency joint venture where officers will work together to provide a comprehensive, all-source-based picture of potential terrorist threats to

191 On August 28, 2004, President Bush announced: "I have ordered the establishment of a national counterterrorism center. This new center builds on the capabilities of the Terrorist Threat Integration Center, … The center will become our government's central knowledge bank for information about known and suspected terrorists, and will help ensure effective joint action across the government so that our efforts against terrorists are unified in priority and purpose. Center personnel will also prepare the daily terrorism threat report that comes to me and to senior government officials." At this writing, no additional details were available. http://www.whitehouse.gov/news/releases/2004/08/20040828.html

U.S. interests. TTIC's structure is designed to ensure rapid and unfettered sharing of relevant information across departmental lines by collapsing bureaucratic barriers and closing interjurisdictional seams. Elements of the DHS, FBI, Central Intelligence Agency (CIA), Department of Defense, and other federal government agencies form TTIC.

> The center is an INTERAGENCY joint venture where officers will work together to provide a comprehensive, all-source-based picture of potential TERRORIST THREATS to U.S. interests.

On a daily basis, TTIC's interagency staff sifts through all-source reporting to identify terrorist plans of tactical concern as well as broader threat themes, which together help guide efforts to disrupt terrorist activities and enhance national security. TTIC also plays a key role in establishing a common threat picture by preparing daily threat assessments and updates for the President and the Departments of Defense, State, and Homeland Security, as well as the broader Intelligence Community, and by creating a consolidated website for the counterterrorism community. The center is colocated with counterterrorism elements from the CIA and FBI, further enhancing coordination efforts.

TTIC is not operational and does not collect intelligence; rather, it receives collected intelligence from other agencies (FBI, CIA, etc.) and analyzes the integrated raw information. While not dealing directly with field components of the FBI or SLTLE, the products disseminated by TTIC serve as an important source for threat development and prevention.

Terrorist Screening Center (TSC)[192]

The TSC was created to ensure that government investigators, screeners, agents, and state and local law enforcement officers have ready access to the information and expertise they need to respond quickly when a suspected terrorist is screened or stopped. The TSC consolidates access to terrorist watch lists from multiple agencies and provide 24/7 operational

192 Information for this section was gained from interviews and reviews of various courses, including testimony and press releases at http://www.fbi.gov/congress/congress04/bucella012604.htm, http://www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm, and http://www.odci.gov/cia/public_affairs/speeches/2003/wiley_speech_02262003.html.

support for thousands of federal screeners and state and local law enforcement officers across the country and around the world. The intent of the TSC is to ensure that federal, state, and local officials are working off of the same unified, comprehensive set of antiterrorist information. Since its implementation on December 1, 2003, the TSC has provided the following:

- A single coordination point for terrorist screening data
- A consolidated 24/7 call center for encounter identification assistance
- A coordinated law enforcement response to federal, state, and local law enforcement
- A formal process for tracking encounters and ensuring that feedback is supplied to the appropriate entities.

The TSC created the terrorist screening database (TSDB), a single, comprehensive source of known or appropriately suspected international and domestic terrorists. These data are available to local, state, and federal law enforcement officers through the National Crime Information Center (NCIC). When a police officer queries the NCIC, he or she may receive a notification that the query resulted in the potential match of a record within the TSDB and the officer is directed to contact the TSC to determine if it is an actual match. If it is an actual match, the TSC transfers the call to the FBI's CT Watch to provide operational guidance to the officer.

Consolidated Terrorist Screening Database

The TSC receives international and domestic terrorist identity records and maintains them in its consolidated TSDB. The TSC reviews each record to determine which are eligible for entry into the NCIC's Violent Gang and Terrorist Organization File (VGTOF) and once the record is entered into NCIC, it is accessible by state, local, and federal law enforcement officers. If a query by a law enforcement officer matches a name in NCIC, the officer will be requested, through the NCIC printout, to contact the TSC. The printout also provides the officer with instructions to arrest, detain, question, or release the subject. If the TSC determines that the person encountered by the officer is a match with a person in the NCIC/VGTOF file, the officer is immediately connected to the FBI's CT Watch for operational

guidance. Depending on the situation, the CT Watch may dispatch a local JTTF agent to assist the law enforcement officer. Information that the officer obtained through the encounter is then sent back to the originating agency.

An example will illustrate the TSC's processes. On August 20, 2004, as two off-duty police officers were traveling across the Chesapeake Bay Bridge, they observed individuals filming the structure of the bridge. The officers reported this suspicious activity to the Maryland Transportation Authority (MTA) who then conducted a traffic stop of the vehicle. The MTA officers ran an NCIC check on one of the occupants of the car and learned that the individual may have a record within the TSDB. At the NCIC's request, the officers contacted the TSC and learned that the individual was the subject of the TSDB record. The TSC transferred the call to the FBI's CT Watch who informed the MTA that the individual an alleged coconspirator in a significant terrorism case. The FBI arrested the subject on a material witness warrant, and a search warrant executed at the subject's residence turned up valuable evidence. This new level of information sharing and cooperation among state, local, and federal law enforcement agencies enhances our ability to prevent a terrorist attack within the United States.

Department of Homeland Security[193]

The DHS, through the Directorate of Information Analysis and Infrastructure Protection (IAIP), will merge the capability to identify and assess current and future threats to the homeland, map those threats against our vulnerabilities, issue timely warnings, and take preventive and protective action.

Intelligence Analysis and Alerts

Actionable intelligence, that is, information that can lead to stopping or apprehending terrorists, is essential to the primary mission of DHS. The timely and thorough analysis and dissemination of information about terrorists and their activities will improve the government's ability to disrupt and prevent terrorist acts and to provide useful warning to the private sector and our population. The IAIP Directorate will fuse and analyze information from multiple sources pertaining to terrorist threats. The DHS

193 The intelligence component of DHS is in the Information Analysis and Infrastructure Protection (IAIP) Directorate: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml. For current information on DHS threats and security, see http://www.dhs.gov/dhspublic/theme_home6.jsp.

will be a full partner and consumer of all intelligence-generating agencies, such as the National Security Agency, the CIA, and the FBI.

The DHS's threat analysis and warning functions will support the President and, as he directs, other national decision makers responsible for securing the homeland from terrorism. It will coordinate and, as appropriate, consolidate the federal government's lines of communication with state and local public safety agencies and with the private sector, creating a coherent and efficient system for conveying actionable intelligence and other threat information. The IAIP Directorate also administers the HSAS.

Critical Infrastructure Protection

The attacks of September 11 highlighted the fact that terrorists are capable of causing enormous damage to our country by attacking our critical infrastructure; food, water, agriculture, and health and emergency services; energy sources (electrical, nuclear, gas and oil, dams); transportation (air, road, rail, ports, waterways); information and telecommunications networks; banking and finance systems; postal services; and other assets and systems vital to our national security, public health and safety, economy, and way of life.

Protecting America's critical infrastructure is the shared responsibility of federal, state, and local government, in active partnership with the private sector, which owns approximately 85 percent of our nation's critical infrastructure. The IAIP Directorate will take the lead in coordinating the national effort to secure the nation's infrastructure. This will give state, local, and private entities one primary contact instead of many for coordinating protection activities within the federal government, including vulnerability assessments, strategic planning efforts, and exercises.

Cyber Security

Our nation's information and telecommunications systems are directly connected to many other critical infrastructure sectors, including banking and finance, energy, and transportation. The consequences of an attack on our cyber infrastructure can cascade across many sectors, causing widespread disruption of essential services, damaging our economy, and

imperiling public safety. The speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. Accordingly, the IAIP Directorate places an especially high priority on protecting our cyber infrastructure from terrorist attack by unifying and focusing the key cyber security activities performed by the Critical Infrastructure Assurance Office (currently part of the Department of Commerce) and the former National Infrastructure Protection Center (FBI). The IAIP Directorate will augment those capabilities with the response functions of the National Cyber Security Division (NCSD) United States Computer Emergency Response Team (US-CERT).[194] Because our information and telecommunications sectors are increasingly interconnected, DHS will also assume the functions and assets of the National Communications System (Department of Defense), which coordinates emergency preparedness for the telecommunications sector.

Indications and Warning Advisories

In advance of real-time crisis or attack, the IAIP Directorate will provide the following:

- Coordinated DHS-FBI threat warnings and advisories against the homeland, including physical and cyber events[195]
- Processes to develop and issue national and sector-specific threat advisories through the HSAS
- Terrorist threat information for release to the public, private industry, or state and local governments.

Figure 11-1 illustrates DHS and intelligence and threat assessment processes. DHS-FBI advisories are produced in several forms. Figures 11-2, 11-3, 11-4, and 11-5 are illustrations of DHS advisory templates. SLTLE agencies have access to these advisories through the various secure law enforcement email systems (i.e., NLETS, LEO, JRIES, Regional Information Sharing Systems [RISS.net], Anti-Terrorism Information Exchange [ATIX]).

194 http://www.us-cert.gov

195 http://www.dhs.gov/dhspublic/verify_redirect.jsp?url=http://www.us-cert.gov&title=cyber+events

Figure 11-1: DHS and Intelligence and Threat Assessment Processes

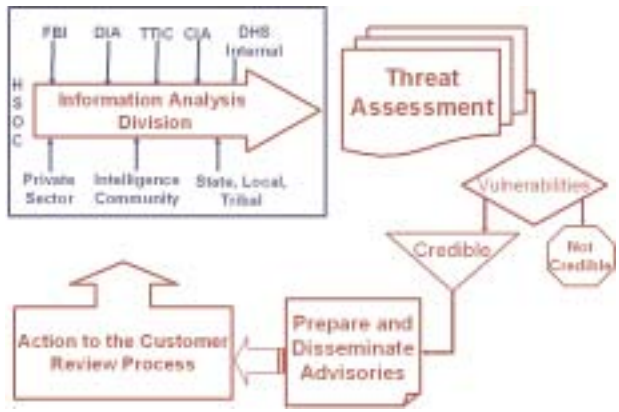

Figure 11-2: DHS Operations Morning Brief

UNCLASSIFIED//FOR OFFICIAL USE ONLY//LAW ENFORCEMENT SENSITIVE

U.S. Department of Homeland Security — Homeland Security Operations Center

WARNING: This document is FOR OFFICIAL USE ONLY. This information shall not be distributed beyond the original addressees without prior authorization of the originator. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

Homeland Security Operations Morning Brief

DD Month YYYY

Overnight Developments

1. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DDMMM,
   HSOC initiated name checks. (CBP Morning Report__Mmm YY; ___; HSOC___)
2. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DDMMM,
   HSOC initiated name checks. (CBP Morning Report__Mmm YY; ___; HSOC___)
3. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DDMMM,
   HSOC initiated name checks. (CBP Morning Report__Mmm YY; ___; HSOC___)
4. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DDMMM,
   HSOC initiated name checks. (CBP Morning Report__Mmm YY; ___; HSOC___)
5. (U//FOUO//LES) STATE: Title. According to CBP reporting, on DDMMM,
   HSOC initiated name checks. (CBP Morning Report__Mmm YY; ___; HSOC___)

Figure 11-3: DHS Information Bulletin

Information Bulletin
Title: _____
Date: _____

LIMITED DISTRIBUTION: **Any release, dissemination, or sharing of this document, or any information contained herein, is not authorized without the express approval of the Department of Homeland Security (DHS). This information is intended for entities identified on the attention line below. All requests for further distribution must be submitted to the DHS Information Management and Requirements Division at 202-282-8168. After business hours contact the DHS Homeland Security Operations Center at Phone (202) 282-8101.**

ATTENTION: Provide guidance as to who within an organization may have primary responsibility for taking action on this product. Examples: Physical Security Officers, Facility Managers, etc.

OVERVIEW
Provide a concise summation of the information in the bulletin, a disclaimer as to the intention of the product, and any limitations as to the further dissemination of this product by the intended recipients.

Homeland Security Information Bulletins are informational in nature and are designed to provide updates on the training, tactics, or strategies of terrorists.

DHS Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

DETAILS
[This section provides the DHS assessment of the information, any recommendations or resultant changes to procedures or processes, and any other applicable information for the consumer.]

SUGGESTED PROTECTIVE MEASURES
[This section provides the DHS recommended protective actions for immediate implementation, including best practices when available.]

Concluding paragraphs:

DHS encourages recipients of this Information Bulletin to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.
DHS intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is _____.

Information Bulletin

Figure 11-4: DHS Physical Advisory

Advisory
Title _____
Date: _____

LIMITED DISTRIBUTION: **Any release, dissemination, or sharing of this document, or any information contained herein, is not authorized without the express approval of the Department of Homeland Security (DHS). This information is intended for entities identified on the attention line below. All requests for further distribution must be submitted to the DHS Information Management and Requirements Division at 202-282-8168. After business hours contact the DHS Homeland Security Operations Center at Phone (202) 282-8101.**

ATTENTION: Provide guidance as to who within an organization may have primary responsibility for taking action on this product. Examples: Physical Security Officers, Facility Managers, etc.

OVERVIEW
Provide one or two sentences in the form of an executive summary of the warning. This may be all a recipient reviews upon initial notification due to the limited storage or viewing capacities of electronic paging devices.

DETAILS
This section provides the DHS assessment of the threat, recommendations and solutions for handling the issue, and any other applicable information for the consumer.

SUGGESTED PROTECTIVE MEASURES

This section provides the DHS recommended protective actions for immediate implementation, including best practices when available.

Concluding paragraphs:

DHS encourages recipients of this Advisory to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.

DHS intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is _____.

Protecting America's CRITICAL INFRASTRUCTURE is the shared responsibility of FEDERAL, STATE, and LOCAL government, in active PARTNERSHIP with the private sector…

Figure 11-5: DHS Cyber Advisory

Advisory
Title: _____
Date: _____

SYSTEMS AFFECTED [Insert list of systems affected by the threat/vulnerability]

OVERVIEW
[Insert a concise synopsis/summary of the threat/vulnerability.]

IMPACT
[The severity of the threat against the affected system(s) depends upon one or more of the following:
- widespread use of the affected system(s)
- mission criticality of the applications running on affected system(s)
- type(s) of affected system(s).

Available analysis of potential or realized impacts will be inserted here.]

DETAILS
[Insert authorized details on the threat/vulnerability.]

SUGGESTED PROTECTIVE MEASURES
DHS is working with other government agencies, network security experts, and industry representatives to define, prioritize, and mitigate these vulnerabilities. DHS encourages implementation of industry best practices. Additionally, the following suggested workarounds and other mitigation steps are provided:

[Insert detailed threat and vulnerability steps including locations for obtaining patches and vulnerability assessments if available.]

Concluding paragraphs:

DHS encourages recipients of this Advisory to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.

DHS intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is _____.

Drug Enforcement Administration[196]

Since its establishment in 1973, the DEA, in coordination with other federal, state, local, and foreign law enforcement organizations, has been responsible for the collection, analysis, and dissemination of drug-related intelligence. The role of intelligence in drug law enforcement is critical. The DEA Intelligence Program helps initiate new investigations of major drug organizations, strengthens ongoing investigations and subsequent prosecutions, develops information that leads to seizures and arrests, and provides policy makers with drug trend information on which they can base programmatic decisions. The specific functions of the DEA's intelligence mission are as follows:

- Collect and produce intelligence in support of the administrator and other federal, state, and local agencies
- Establish and maintain close working relationships with all agencies that produce or use narcotics intelligence
- Increase the efficiency in the reporting, analysis, storage, retrieval, and exchange of such information;
- Undertake a continuing review of the narcotics intelligence effort to identify and correct deficiencies.

196 A number of DEA Strategic Intelligence Reports are available online at http://www.dea.gov/pubs/intel.htm. For other intelligence reports and related information, contact your nearest DEA Field Office http://www.dea.gov/agency/domestic.htm#caribbean.

The DEA's Intelligence Program has grown significantly since its inception. From only a handful of intelligence analysts (I/A) in the domestic offices and Headquarters in 1973, the total number of intelligence analysts worldwide is now more than 680. DEA's intelligence Program consists of several entities that are staffed by both intelligence analysts and special agents: Intelligence groups and functions in the domestic field divisions, district, resident and foreign offices, the El Paso Intelligence Center, and the Intelligence Division at DEA Headquarters. Program responsibility for the DEA's intelligence mission rests with the DEA assistant administrator for intelligence.

Legislation and presidential directives and orders have expanded the role of the Intelligence Community and the Department of Defense in the anti-drug effort. DEA interaction with both components occurs on a daily basis in the foreign field and at Headquarters. At the strategic intelligence level, the Intelligence Division participates in a wide range of interagency assessment and targeting groups that incorporate drug intelligence from the antidrug community to provide policymakers with all-source drug trend and trafficking reporting.

With analytical support from the Intelligence Program, DEA has disrupted major trafficking organizations or put them entirely out of business. The DEA Intelligence Division also cooperates a great deal with state and local law enforcement and will soon provide intelligence training for state, local, federal, and foreign agencies. This training will be held at the Justice Training Center in Quantico, Virginia, and will address the full spectrum of drug intelligence training needs. The best practices and theories of all partners in working the drug issue will be solicited and incorporated into the training. Academic programs, the exchange of federal, state, and local drug experience, and the sharing of, and exposure to, new ideas will result in more effective application of drug intelligence resources at all levels. The DEA divides drug intelligence into three broad categories: tactical, investigative, and strategic.

- Tactical intelligence is evaluated information on which immediate enforcement action – arrests, seizures, and interdictions – can be based.
- Investigative intelligence provides analytical support to investigations and prosecutions to dismantle criminal organizations and gain resources.
- Strategic intelligence focuses on the current picture of drug trafficking from cultivation to distribution that can be used for management decision making, resource deployment, and policy planning.

Intelligence Products

Tactical and investigative intelligence is available to SLTLE agencies through the local DEA field office. In addition, intelligence can be shared with state, local, and tribal agencies through secure email. Many strategic intelligence reports are available on the DEA website.[197] Reports that are "Law Enforcement Sensitive" can be obtained through the local DEA office.

197 See http://www.usdoj.gov/dea/pubs/intel.htm.

El Paso Intelligence Center (EPIC)[198]

The El Paso Intelligence Center (EPIC) was established in 1974 in response to a Department of Justice study. The study, which detailed drug and border enforcement strategy and programs, proposed the establishment of a southwest border intelligence service center staffed by representatives of the Immigration and Naturalization Service, the U.S. Customs Service, and the DEA. The original EPIC staff comprised 17 employees from the three founding agencies. Initially, EPIC focused on the U.S.-Mexico border and its primary interest was drug movement and immigration violations.

Today, EPIC still concentrates primarily on drug movement and immigration violations. Because these criminal activities are seldom limited to one geographic area, EPIC's focus has broadened to include all of the United States and the Western Hemisphere where drug and alien movements are directed toward the United States. Staffing at the DEA-led center has increased to more than 300 analysts, agents, and support personnel from 15 federal agencies, the Texas Department of Public Safety, and the Texas Air National Guard. Information-sharing agreements with other federal law enforcement agencies, the Royal Canadian Mounted Police, and each of the 50 states ensure that EPIC support is available to those who need it. A telephone call, fax, or email from any of these agencies provides the requestor with real-time information from different federal databases, plus EPIC's own internal database.

198 See http://www.dea.gov/programs/epic.htm.

In addition to these services, a number of EPIC programs are dedicated to post-seizure analysis and the establishment of links between recent enforcement actions and ongoing investigations. EPIC also coordinates training for state and local officers in the methods of highway drug and drug currency interdiction through its Operation Pipeline program. In addition, EPIC personnel coordinate and conduct training seminars throughout the United States, covering such topics as indicators of trafficking and concealment methods used by couriers.

In a continuing effort to stay abreast of changing trends, EPIC has developed the National Clandestine Laboratory Seizure Database. EPIC's future course will be driven by the National General Counterdrug

Intelligence Plan, as well. As a major national center in the new drug intelligence architecture, EPIC will serve as a clearinghouse for the High-Intensity Drug Trafficking Areas (HITDA) Intelligence Centers, gathering state and local law enforcement drug information and providing drug intelligence back to the HIDTA Intelligence Centers.

National Drug Pointer Index (NDPIX) and National Virtual Pointer System (NVPS)[199]

For many years, state and local law enforcement envisioned a drug pointer system that would allow them to determine if other law enforcement organizations were investigating the same drug suspect. The DEA was designated by the Office of National Drug Control Policy in 1992 to take the lead in developing a national drug pointer system to assist federal, state, and local law enforcement agencies investigating drug trafficking organizations and to enhance officer safety by preventing duplicate investigations. The DEA drew from the experience of state and local agencies to make certain that their concerns were addressed and that they had extensive input and involvement in the development of the system.

199 See http://www.dea.gov/programs/ndpix.htm.

The National Law Enforcement Telecommunications System (NLETS)-a familiar, fast, and effective network that reaches into almost every police entity in the United States-is the backbone of the NDPIX.

The National Drug Pointer Index (NDPIX) became operational across the United States in October 1997. The National Law Enforcement Telecommunications System (NLETS)–a familiar, fast, and effective network that reaches into almost every police entity in the United States–is the backbone of the NDPIX. Participating agencies are required to submit active case-targeting information to NDPIX to receive pointer information from the NDPIX. The greater the number of data elements entered, the greater the likelihood of identifying possible matches. Designed to be a

true pointer system, the NDPIX merely serves as a "switchboard" that provides a vehicle for timely notification of common investigative targets. The actual case information is shared only when telephonic contact is made between the officers or agents who have been linked by their entries into the NDPIX.

NDPIX was developed to: (1) promote information sharing; (2) facilitate drug-related investigations; (3) prevent duplicate investigations; (4) increase coordination among federal, state, and local law enforcement agencies; and (5) enhance the personal safety of law enforcement officers. At this writing, NDPIX is being transitioned and upgraded to the National Virtual Pointer System (NVPS). A steering committee–which included DEA, HIDTA, RISS, the National Drug Intelligence Center (NDIC), the National Institute of Justice (NIJ), the National Sheriff's Association (NSA), the International Association of Chiefs of Police (IACP), and the National Alliance of State Drug Enforcement Agencies (NASDEA)–developed the specifications for the system and is overseeing its testing and transition.

Characteristics of the NVPS will include the following:

- It will cover all crimes, not just drugs.
- The system will accept only targets of open investigations with assigned case numbers.
- Transaction formats will contain an identifying field for the NVPS Identifier.
- It will use a secure telecommunications network.
- It will use the NDPIX "Mandatory" data elements.
- A single sign-on from any participant will allow access to all participating pointer databases.
- Each system will provide a userid and password to its respective users.
- Each system will maintain its own data.
- Uniform Crime Reporting (UCR) or the National Incident-Based Reporting System (NIBRS) codes will be used to identify type of crime.
- The system will target deconfliction for all crimes.
- It will rely on web-based communications.
- NVPS will have links with HIDTA and RISS.

An important aspect of the links with NVPS will be that NDPIX participants will continue to use their existing formats and procedures for entries, updates, and renewals and NDPIX notifications will continue in the same formats. The transition to NVPS will be seamless. This change represents an important upgrade to networked intelligence that can be of value to all law enforcement agencies.

National Drug Intelligence Center (NDIC)[200]

The National Drug Intelligence Center (NDIC), established in 1993, is a component of the U.S. Department of Justice and a member of the Intelligence Community. The General Counterdrug Intelligence Plan, implemented in February 2000, designated NDIC as the nation's principal center for strategic domestic counterdrug intelligence. The intent of NDIC is to meet three fundamental missions:

- To support national policymakers and law enforcement decision makers with strategic domestic drug intelligence
- To support Intelligence Community counterdrug efforts
- To produce national, regional, and state drug threat assessments.

The Intelligence Division consists of six geographic units and four specialized units. The six geographic units correspond to the regions of the Department of Justice Organized Crime Drug Enforcement Task Force (OCDETF)[201] program and concentrate on drug trafficking and abuse. The four specialized units include the Drug Trends Analysis Unit, the Organized Crime and Violence Unit, the National Drug Threat Assessment Unit, and the National Interdiction Support Unit.

Within the geographic units, NDIC intelligence analysts cover each state and various U.S. territories. Intelligence analysts maintain extensive contacts with federal, state, and local law enforcement and Intelligence Community personnel in all 50 states, the District of Columbia, Puerto Rico, the Virgin Islands, and the Pacific territories of Guam, American Samoa, and the Northern Mariana Islands. NDIC collaborates with other agencies such as the DEA, FBI, U.S. Coast Guard, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Bureau of Prisons, and the Office of

200 See http://www.usdoj.gov/ndic/.

201 While the OCDETFs are operational, not intelligence entities, they are not only consumers of intelligence, but are also sources for information collection. For more information see http://www.usdoj.gov/dea/programs/ocdetf.htm.

National Drug Control Policy (ONDCP). NDIC is one of four national intelligence centers including the EPIC, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), and the DCI Crime and Narcotics Center (CNC). NDIC also works closely with the High Intensity Drug Trafficking Areas (HIDTAs) and the OCDETF.

Intelligence Products

Threat assessments, NDIC's primary intelligence products, provide policy makers and counterdrug executives with timely, predictive reports of the threat posed by illicit drugs in the United States.

- The ***National Drug Threat Assessment***, NDIC's major intelligence product, is a comprehensive annual report on national drug trafficking and abuse trends within the United States. The assessment identifies the primary drug threat to the nation, monitors fluctuations in consumption levels, tracks drug availability by geographic market, and analyzes trafficking and distribution patterns. The report highlights the most current quantitative and qualitative information on availability, demand, production and cultivation, transportation, and distribution, as well as the effects of a particular drug on abusers and society as a whole.
- ***State Drug Threat Assessment*** provides a detailed threat assessment of drug trends within a particular state. Each report identifies the primary drug threat in the state and gives a detailed overview of the most current trends by drug type.
- ***Information Bulletins*** are developed in response to new trends or high-priority drug issues. They are relayed quickly to the law enforcement and intelligence communities and are intended to warn law enforcement officials of emerging trends.

High-Intensity Drug Trafficking Areas (HIDTA) Regional Intelligence Centers[202]

The HIDTA Intelligence System has more than 1,500 law enforcement personnel, mostly criminal intelligence analysts, participating full time in more than 60 intelligence initiatives in the 28 HIDTA designated areas

202 See http://www.whitehousedrugpolicy.gov/hidta/ for HIDTA points of contact.

throughout the United States. While HIDTA is a counterdrug program, the intelligence centers operate in a general criminal intelligence environment, thereby leveraging all criminal intelligence information for the program's primary mission.[203]

The HIDTA Intelligence System, a core element in the creation and growth of many SLTLE intelligence programs, largely depends on HIDTA program mandates. Each HIDTA must establish an intelligence center comanaged by a federal and a state or local law enforcement agency. The core mission of each individual HIDTA Intelligence Center is to provide tactical, operational, and strategic intelligence support to its HIDTA executive board, a group of participating law enforcement agency principals responsible for the daily management of their respective HIDTAs, HIDTA-funded task forces, and other regional HIDTAs. Developing regional threat assessments and providing event and target deconfliction are also among the centers' core missions. These core functions are critical to building trust and breaking down parochialism between and among the local, state, and federal participating law enforcement agencies.

The plan to connect all HIDTA Intelligence Centers through RISS.net was initiated by the HIDTA Program Office at ONDCP in 1999 and completed in mid-2003. The HIDTA Program Office has commissioned interagency and interdisciplinary working committees to develop a national information-sharing plan, focusing on issues relating to legal, agency policy, privacy, technical, and logistical information-sharing matters. HIDTA program and committee personnel are coordinating with, and implementing recommendations made by, other information-sharing initiatives such as Global, Matrix, and federally sponsored intelligence programs.[204]

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)[205]

The Intelligence Division of ATF has evolved rapidly as an important tool for the diverse responsibilities of the bureau. Several activities in particular demonstrate the intelligence capability and resources of ATF.

203 http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=139&issue_id=11200

204 As an illustration of the comprehensive and integrated nature of the HIDTA programs and intelligence centers, see http://www.ncjrs.org/ondcppubs/publications/enforce/hidta2001/ca-fs.html.

205 Contact your local ATF Field Office for Intelligence Products and resources. Offices and contact information can be found at http://www.atf.gov/field/index.htm.

The ATF, which is now an agency of the Department of Justice, has developed Field Intelligence Groups at each of its 23 Field Divisions strategically located throughout the United States. These intelligence groups meld the training and experience of special agents, intelligence research specialists, industry operations inspectors, and support staff who focus on providing tactical intelligence support for their respective field divisions and their external law enforcement partners. Each Field Intelligence Group works under the authority of a supervisory special agent. The intelligence group supervisors are coordinated by, and work in conjunction with, the Intelligence Division to form a bureau-wide intelligence infrastructure. The Intelligence Division has provided indoctrination and training for all Field Intelligence Group supervisors, intelligence officers, and intelligence research specialists.

... the [ATF] Intelligence Division spearheaded the formulation of an MOU with the FBI to collaborate on investigations conducted by JOINT TERRORISM TASK FORCES located throughout the United States.

ATF maintains intelligence partnerships with the NDIC, EPIC, FinCEN, INTERPOL, the Federal Bureau of Investigation Counter Terrorism Center, (FBI/CTC) and other international intelligence sources. Furthermore, ATF maintains a memorandum of understanding (MOU) with the six Regional Information Sharing Systems (RISS) that represent thousands of SLTLE agencies, pledging to share unique and vital intelligence resources. These external partners are key components of ATF's Strategic Intelligence Plan and the means by which ATF ensures a maximum contribution to the nation's law enforcement and intelligence communities.

During FY 2000, the Intelligence Division spearheaded the formulation of an MOU with the FBI to collaborate on investigations conducted by Joint Terrorism Task Forces located throughout the United States. This MOU brings ATF's unique knowledge and skills of explosives and firearms violations to the FBI's expertise in terrorism.

The Intelligence Division has implemented a state-of-the-art automated case management/ intelligence reporting system called N-FOCIS (National Field Office Case Information System). The system consists of two companion applications: N-FORCE for special agents and N-SPECT for industry operations inspectors. Both eliminate redundant manual data entry on hard copy forms and provide a comprehensive reporting and information management application in a secure electronic environment.

N-FOCIS constitutes an online case management system and electronic central information repository that allows ATF to analyze and fully exploit investigative intelligence. N-FOCIS epitomizes the strength and unique value of ATF's combined criminal and industry operations enforcement missions. The Intelligence Division has provided in-service training to many of the ATF field division special agents, investigative assistants, and inspectors on the use of the N-FOCIS applications. ATF is planning to expand the N-FOCIS functionality and to integrate N-FOCIS with several key ATF applications including the National Revenue Center, the National Tracing Center, National Arson and Explosive Repository, and the Intelligence Division's Text Management System. This integration plan establishes N-FOCIS as the bureau's information backbone.

The Intelligence Division prepares a wide range of strategic intelligence reports related to the ATF mission that are available to SLTLE. In addition, intelligence is shared with state and local agencies through RISS and the JTTFs. In addition, ATF will readily respond to inquiries wherein SBU information may be shared.

ATF has also created a series of Regional Crime Gun Centers. The intent of the centers is to integrate gun tracing with ATF intelligence as well as with the HIDTA Regional Intelligence Centers to suppress gun-related crime .[206]

Financial Crimes Enforcement Network (FinCEN)[207]

The Financial Crimes Enforcement Network (FinCEN) is a network designed to bring agencies, investigators, and information together to fight the complex problem of money laundering. Since its creation in 1990, FinCEN

206 As an illustration see http://www.atf.gov/field/newyork/rcgc/index.htm.

207 See http://www.fincen.gov/.

has worked to maximize information sharing among law enforcement agencies and its other partners in the regulatory and financial communities. Through cooperation and partnerships, FinCEN's network approach encourages cost-effective and efficient measures to combat money laundering domestically and internationally.

The network supports federal, state, local, tribal, and international law enforcement by analyzing information required under the Bank Secrecy Act (BSA), one of the nation's most important tools in the fight against money laundering. The BSA's record keeping and reporting requirements establish a financial trail for investigators to follow as they track criminals, their activities, and their assets. Over the years, FinCEN staff has developed its expertise in adding value to the information collected under the BSA by uncovering leads and exposing unknown pieces of information contained in the complexities of money laundering schemes.

Illicit financial transactions can take many routes – some complex, some simple, but all increasingly inventive – with the ultimate goal being to disguise its source. The money can move through banks, check cashers, money transmitters, businesses, casinos, and is often sent overseas to become "clean." The tools of the money launderer can range from complicated financial transactions, carried out through webs of wire transfers and networks of shell companies, to old-fashioned currency smuggling.

Intelligence research specialists and law enforcement support staff research and analyze this information and other critical forms of intelligence to support financial criminal investigations. The ability to network with a variety of databases provides FinCEN with one of the largest repositories of information available to law enforcement in the country. Safeguarding the privacy of the data it collects is an overriding responsibility of the agency and its employees-a responsibility that strongly imprints all of its data management functions and operations.

FinCEN's information sources fall into three categories:

- ***Financial Database:*** The financial database consists of reports that the BSA requires to be filed, such as data on large currency transactions

conducted at financial institutions or casinos, suspicious transactions, and international movements of currency or negotiable monetary instruments. This information often provides invaluable assistance for investigators because it is not readily available from any other source and preserves a financial paper trail for investigators to track criminals' proceeds and their assets.

- ***Commercial Databases:*** Information from commercially available sources plays an increasingly vital role in criminal investigations. Commercial databases include information such as state, corporation, property, and people locator records, as well as professional licenses and vehicle registrations.
- ***Law Enforcement Databases:*** FinCEN is able to access various law enforcement databases through written agreements with each agency.

FinCEN works closely with the International Association of Chiefs of Police (IACP), National Association of Attorneys General (NAAG), National White Collar Crime Center (NW3C), and other organizations to inform law enforcement about the information that is available at FinCEN and how to use that information to attack criminal proceeds.

208 See http://www.fincen.gov/le_hifcadesign.html.

High Risk Money Laundering and Related Financial Crimes Areas (HIFCA)[208]

HIFCAs were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the federal, state, and local levels in highintensity money laundering zones. HIFCAs may be defined geographically or they can also be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.

The HIFCA program is intended to concentrate law enforcement efforts at the federal, state, and local levels to combat money laundering in designated high-intensity money laundering zones. To implement this goal, a money laundering action team will be created or identified within each HIFCA to spearhead a coordinated federal, state, and local antimoney laundering effort. Each action team will: (1) be composed of all relevant

federal, state, and local enforcement authorities, prosecutors, and financial regulators; (2) focus on tracing funds to the HIFCA from other areas, and from the HIFCA to other areas so that related investigations can be undertaken; (3) focus on collaborative investigative techniques, both within the HIFCA and between the HIFCA and other areas; (4) ensure a more systemic exchange of information on money laundering between HIFCA participants; and (5) include an asset forfeiture component as part of its work.

Gateway

FinCEN's Gateway system enables federal, state, and local law enforcement agencies to have online access to records filed under the BSA. The system saves investigative time and money by enabling investigators to conduct their own research and analysis of BSA data rather than relying on the resources of an intermediary agency to obtain financial records. A unique feature of Gateway is the "query alert" mechanism that automatically signals FinCEN when two or more agencies have an interest in the same subject. In this way, FinCEN is able to assist participating agencies in coordinating their investigations.

Virtually every criminal enterprise and terrorist organization is involved in some dimension of money laundering. The complexities of forensic accounting, often complicated by jurisdictional barriers, reinforces the need for intelligence personnel to be aware of the resources and expertise available through FinCEN.

CONCLUSION

As demonstrated in this chapter, the amount of information and intelligence being generated by federal law enforcement agencies is significant. If that information is not being used, then its value is lost. Not only are federal agencies responsible for making information available to SLTLE agencies in an accessible and consumable form, nonfederal law enforcement must develop the mechanisms for receiving the information and to be good consumers of it.

One of the ongoing controversies is the problem of dealing with classified information. This chapter explained the classification process as well as the initiatives that are being undertaken to deal with this issue. One measure is to increase the number of security clearances for SLTLE personnel. The other measure is for the FBI to write intelligence reports so that they are unclassified, but remain Law Enforcement Sensitive (LES) in order to give SLTLE personnel access.

By gaining access to secure networking (e.g., LEO, RISS.net, ATIX, JRIES), interacting on a regular basis with the FBI Field Intelligence Group (FIG), and proactively interacting with other federal law enforcement intelligence offices, SLTLE can have access to the types of critical intelligence necessary to protect their communities.