HOMELAND SECURITY:
Intelligence Guide for Fire Chiefs

A reference guide for Fire Chiefs to assist them in acquiring
a basic understanding of how Homeland Security
and the Fire Service can work together.

IAFC

INTERNATIONAL
FIRE CHIEFS
ASSOCIATION
ORG 1873

Homeland Security
Intelligence Guide for Fire Chiefs
Table of Contents

Homeland Security

Intelligence Guide for Fire Chiefs

Introduction

Since the terrorist attacks of September 11, 2001, fire chiefs across the United States have been seeking intelligence and information about the terrorism threat to their communities in order to assist in eliminating or reducing the element of strategic surprise in their operations. Fire chiefs have been primarily interested in receiving intelligence on terrorism trends and targeting related to critical infrastructure and special events in their jurisdictions.

This intelligence has been sought to enhance the situational awareness and safety of first responders, incident commanders and field operators. Many fire chiefs have struggled to identify a reliable source of terrorism threat intelligence that can address the specific needs of their jurisdictions and fire service operations.

While the needs and resources within every jurisdiction are unique, this guide will describe possible options that fire chiefs may explore for accessing the intelligence they require.

Chapter 1: Intelligence

While our information sharing capabilities have improved significantly, substantial obstacles remain. We must continue to break down information barriers among federal, state, local, and tribal partners and the private sector.

-2007 National Strategy for Homeland Security

Basic intelligence is the fundamental and factual reference material on a country or issue. It depicts the fundamental intelligence pertaining to the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas. Such intelligence can be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. It serves as the foundation for current and estimative intelligence.[1]

The United States has over one million firefighters serving in over 30,000 fire departments that respond to over 24 million emergencies annually**.** In their efforts to prevent and respond to life and property loss, firefighters enter homes, businesses, vehicles, and other assets, without a search warrant, thousands of times each day. This access has allowed firefighters to identify potential terrorist activities, oftentimes unexpectedly for both the firefighters and the potential terrorists. U.S. firefighters may be in a unique position to positively or negatively impact our current homeland security information-sharing efforts.[2]

---

[1] U.S. Legal Definitions: Basic Intelligence Law & Legal Definition, www.uslegal.com
[2] Heirston, Firefighters and Information Sharing. *Homeland Security Affairs,* Volume VI, No. 2 (May 2010) www.hsaj.org

As few as fifteen of the 30,000 U.S. fire departments formally use terrorism indicators and communicate the information gathered to the homeland security community. Despite the obvious potential benefit of thousands of firefighters as consumers and collectors of information, the current information-sharing environment is *ad hoc* at best and in many locales, non-existent. It appears few firefighters have received formal training in what terrorist indicators to look for or how to communicate or request information. One aspect of determining whether information collected by a firefighter is legal or the *fruit of a poisonous tree* may lie in whether the firefighter identified potential terrorist-related items or information during the normal course of their duty or the firefighter was assigned to collect information on suspected terrorists.[3]

The second edition of the ***Interagency Threat Assessment and Coordinating Group (ITACG) Intelligence Guide for First Responders*** provides an excellent overview of the Intelligence Community. In addition, it provides information regarding resources available to state, local, and tribal partners, and guidance on understanding federal intelligence reporting, terminology and acronyms. This version updates the first edition, which was published in October 2009, and includes two new sections: "Reporting Suspicious Activity," which covers participation in the Nationwide Suspicious Activity Reporting Initiative and "Joint Partnerships," which highlights a few of the joint federal and state, local and tribal activities around the country. For complete information on this guide, visit the ITACG Intelligence Guide for First Responders.

---

[3] Heirston, Firefighters and Information Sharing. *Homeland Security Affairs,* Volume VI, No. 2 (May 2010) www.hsaj.org

A cooperative agreement between the IAFC and ITACG has fire service personnel participating within ITACG by detailing members to Washington, DC, to work there in an effort to provide fire service interpretation to the raw information coming in at a classified level. This is critical in making certain that the needs of the fire service are clearly known and defined. This will identify what information should be provided to the local fire service leaders.

Fire Service Intelligence Enterprise (FSIE)

The Fire Service Intelligence Enterprise initiative is a national strategic approach to information sharing between the U.S. fire service and homeland security community. Homeland security affiliates for the FSIE were identified within the FSIE framework as federal, state, local, tribal, and private sector "agencies or organizations that are stakeholders of FSIE initiatives, either as collaborators or customers" for the DHS. The FSIE Concept of Operations Plan (FSIE CONPLAN) appears to be a strategic extension and formal expansion of the current informal fire service information-sharing environment between the fire service and homeland security communities. The primary FSIE CONPLAN venues for sharing information are federal, state, and local fusion centers. Working within the Global Justice Information Sharing Initiative, fire service fusion center liaisons or representatives would act as nodes, and the fusion centers would act as hubs for receiving and disseminating relevant information in a timely and actionable manner.[4]

---

[4] Heirston, Firefighters and Information Sharing. *Homeland Security Affairs,* Volume VI, No. 2 (May 2010) www.hsaj.org

Chapter 2: How to Obtain Information: Partnerships, Resources and Alerts

Partnerships

Before intelligence analysts and managers can provide decision-makers with intelligence that they actually need to make informed resource decisions on appropriate strategic, operational and tactical mitigation actions, they must first understand the consumers' intelligence requirements. An intelligence requirement in this context can be defined as a requirement for intelligence to fill a gap in the knowledge or understanding of the operational environment – before, during, and after an incident.[5]

The first step for a fire chief seeking intelligence about the threat of terrorism is to become an advocate for their department's needs. There are three common places a fire chief could seek terrorism threat intelligence: Fusion Centers, Joint Terrorism Task Forces (JTTF), and local law enforcement agencies. Each fire chief will have to evaluate their local landscape to determine how to best engage each of these sources to request assistance.

Fusion Centers

State and major fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related

---

[5] Townsend, Keely; Sulivan, John P.; Monahan, Thomas; and Donnelly, John (2010) "Intelligence-Led Mitigation," Journal of Homeland Security and Emergency Management: Vol.7 :Iss.1 Article 63

information between the federal government and state, local, tribal, territorial and private sector partners.

Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line fire service, law enforcement, public safety, emergency response, public health, critical infrastructure and key resources (CIKR) protection, and private security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities. They provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. In addition, they conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, and connectivity to federal systems, technology, and grant funding.

There are two types of fusion centers: *all hazard* and *law enforcement-centric*. Law enforcement centers are not familiar with fire service needs and generally do not interact with fire service personnel. This issue can create a situation whereby the intelligence information is not always made available to the fire service which is critical to the safety of our members and our operations in support of protecting the public.

Because of their position in the Intelligence Community and their legislated relationship with local government, the first source of terrorism threat intelligence for a fire chief is a state and local Fusion Center.[6] Many of the fusion centers will not directly share *classified information* with the fire service or other discipline personnel if they do not have a clearance level with one of the federal agencies: U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), U.S. Department of Defense (DOD), U.S. Department of Energy (DOE), etc. This can be a major stumbling block if the law enforcement personnel at the state and local level do not know how to create a tear line for the information to be passed.

The Fusion Center's guide for interacting with the fire service is the Fire Service Integration for Fusion Centers: An appendix to the Baseline Capabilities for State and Major Urban Fusion Centers. The document describes the value and importance of incorporating the fire service into the fusion process and identifies it as a pivotal step for the fire service in developing meaningful relationships with Fusion Centers. The fire chief can use this document to identify recommended actions and guidance to effectively integrate the fire service into the fusion process.[7]

Contact information for fire service participation in state and local Fusion Centers can be supplied by the Fire Service Intelligence Liaison, Critical Infrastructure Program Manager, and U.S. Fire Administration.

---

[6] U.S. Department of Homeland Security, "State and Local Fusion Centers," http://www.dhs.gov/files/programs/gc_1156877184684.shtm (accessed 24 July 2012).
[7] U.S. Department of Homeland Security, "Fire Service Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers," April 2010 http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

Joint Terrorism Task Force (JTTF)

The second source of terrorism threat intelligence for a fire chief is the FBI's Joint Terrorism Task Force (JTTF) operating in their community. "JTTFs are small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. It is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement."[8] Because the JTTFs are integral to the successful mitigation and investigation of a terrorism related incident, it is important for the fire chief to have developed a relationship with the JTTF prior to an incident occurring. In some areas of the country, members of the fire department may serve as members of the JTTF. The JTTF can be contacted through your local FBI Field Office.

Local Law Enforcement

The third source of terrorism threat intelligence is the most important source of intelligence – your local law enforcement agency. This source is the most important, because local officials know their area best and many already have relationships with Fusion Centers and the JTTFs. A fire chief should take advantage of establishing relationships with local law enforcement officials long before a threat or disaster occurs in their community. These relationships will allow the easy flow of information during a crisis, which is

---

[8] U.S. Department of Justice, "Joint Terrorism Task Forces," http://www.justice.gov/jttf/ (Accessed 18 October 2010)

especially important when firefighter safety may be contingent on the fire official receiving important information prior to placing firefighters in a dangerous position. Engaging the local law enforcement agency about the intelligence needs of the fire service allows the fire chief to create a dialogue for effectively supporting terrorism threat intelligence sharing at the local level. Learn who they are and become friends with your local Police Chief, Sheriff, State Police Chief, FBI and Alcohol Tobacco and Firearms Bureau (ATF).

Information Sharing Portals and Systems

There are multiple information sources available to fire chiefs and their staff that provide intelligence and information. To properly put this information in context, the fire chief must understand the systems, their purpose and their audience. The most important point to remember regarding these systems is that they are not used to disseminate imminent threat information. Imminent threat information will flow through local law enforcement. These systems are primarily to provide information about terrorism tactics.

Homeland Security Information Network

The Homeland Security Information Network (HSIN) is a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. HSIN is made up of a growing network of communities called Communities of Interest (COI). COIs are organized by state organizations, federal

organization or mission areas, and include emergency management, law enforcement, critical sectors, intelligence, etc. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging and document sharing. HSIN allows partners to work together instantly regardless of their location, to communicate, collaborate, and coordinate.

Membership in HSIN is COI-based. To become a member, first decide which COI(s) meet your needs such as critical sectors, emergency management, intelligence, homeland security and multi- mission. If you need additional information, please contact the Mission Advocate listed as the point of contact for a particular COI, or email the HSIN program at HSIN.Outreach@HQ.DHS.gov.

Once you have identified the COI of interest to you, you will need to be nominated and vetted into the COI. This process will require that you provide the following information on the HSIN membership application:

- Name
- A valid email address
- Department/Organization
- Supervisor
- Valid Contact Information

You may obtain an application by sending a request to the above HSIN address. Once nominated, the COI Validating Authority will review your membership application and approve or deny your admission to the COI. If

the application is approved, an email will be sent to you with instructions on how to log into HSIN for the first time.

Law Enforcement Online

Law Enforcement Online (LEO) is a secure, Internet-based communications portal for law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. LEO catalyzes and strengthens collaboration and information sharing by providing access to sensitive but unclassified information and various state-of-the-art communications services and tools. It is available to vetted users anywhere in the world around-the-clock and is offered free of charge to members.

LEO started in 1995 as a small dial-up service with just 20 members. Now, it has more than 100,000 members across the world and a host of features and capabilities offered through a Virtual Private Network on the Internet. LEO offers the following services:

- A national alert system directing members to the LEO site for information on emergencies (e.g., the London bombings)
- Some 1,100 Special Interest Groups (SIG) which allow members who share expertise or interests to connect with each other, including sections on terrorism, street gangs, and bombs
- Access to important and useful databases, like those run by the National Center for Missing and Exploited Children

- Email services, which enable members to submit fingerprints to the FBI for processing by Integrated Automated Fingerprint Identification System

- A Virtual Command Center – an information sharing and crisis management tool that allows the law enforcement community to use LEO at local and remote sites as an electronic command center to submit and view information and intelligence

- Distance learning, with several online learning modules on topics like terrorism response, forensic anthropology, and leadership

- A multimedia library of publications, documents, studies, research, technical bulletins, and other reports of interest to LEO users

If you work for a law enforcement, criminal justice, or public safety agency, you can join LEO. Just send an email to leoprogramoffice@leo.gov .

Technical Resource for Incident Prevention

The Technical Resource for Incident Prevention (TRIPwire) is the Department of Homeland Security's 24/7 online, secure, collaborative, information sharing network for bomb squad, law enforcement, and other emergency services personnel to learn about current terrorist improvised explosive device (IED) tactics, techniques, and procedures, including design and emplacement considerations. It was developed and maintained by the Office of Infrastructure Protection's Office for Bombing Prevention.

TRIPwire combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to help law enforcement anticipate, identify, and prevent IED incidents. It is a secure, restricted-access information sharing network. TRIPwire is provided free of charge only to members of the bombing prevention community.

National Terrorism Advisory System (NTAS)

Terrorism information and intelligence is based on the collection, analysis and reporting of a range of sources and methods. While intelligence may indicate that a threat is credible, specific details may still not be known. As such, fire departments should continue to stay informed and vigilant throughout the duration of an NTAS Alert. Each alert provides information to the public about the threat. This information includes, if available, the geographic region, mode of transportation, or critical infrastructure potentially affected by the threat. In addition, the information provides protective actions being taken by authorities and steps that individuals and communities may take to protect themselves and their families, to help prevent, mitigate or respond to the threat.

Fire departments should report suspicious activity to their local law enforcement authorities. The *If You See Something, Say Something*™ campaign across the United States encourages all citizens to be vigilant for indicators of potential terrorist activity and to follow NTAS Alerts for information about threats in specific places or for individuals exhibiting certain types of suspicious activity.

The NTAS system has two levels of alerts:

Imminent Threat Alert	Warns of a credible, specific, and impending terrorist threat against the United States.
Elevated Threat Alert	Warns of a credible terrorist threat against the United States.

After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other Federal entities, whether an NTAS Alert should be issued. NTAS Alerts will be issued when credible information is available.

These alerts will include a clear statement that there is an imminent threat or elevated threat. Using available information, the alerts will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses and government can take to help prevent, mitigate or respond to the threat.

The NTAS Alerts will be based on the nature of the threat. In some cases, alerts will be sent directly to law enforcement or affected areas of the private sector. In other situations, alerts will be issued more broadly to the American people through both official and media channels.

Chapter 3: Reporting Information

Suspicious Activity Reporting

Suspicious Activity Reporting (SAR) creates implementation and policy challenges for fire chiefs because many fire service personnel view this responsibility as a law enforcement activity. However, fire service constituents should collaborate with Fusion Centers to develop outreach materials for fire service personnel on recognizing and reporting behaviors and incidents indicative of criminal activity associated with international and domestic terrorism. In addition, the fire department should collaborate with the Fusion Centers to support and/or develop training for fire service personnel to identify and appropriately report suspicious activities, indicators, warnings, and the associated privacy and civil rights/civil liberty protection requirements.

Nationwide SAR Initiative

The Nationwide Suspicious Activity Reporting Initiative (NSI) is an administration-wide effort to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism related suspicious activities. NSI is implemented in partnership with state and local officials across the nation and is led by the U.S. Department of Justice.

Every day, first responders at all levels of government -- state, local, tribal and federal -- observe suspicious behaviors or receive such reports from

concerned civilians, private security and other government agencies. What might not seem significant (e.g., taking pictures of a ferry during loading), when combined with other actions and activity, may become a composite indicating the possibility of criminal – even terrorist – activity.

Traditionally, street officers have had little to do with counterterrorism. After the terrorist attacks of September 11, 2001, it became obvious that al Qaeda members had prepared not only in far off Afghan training camps, but also in Minnesota and flight schools in Florida. Therefore, in today's policing, "connecting the dots" of suspicious activity before an incident occurs has become an integral and imperative job for America's law enforcement. This includes the officer on the street, the supporting analysts and the emergency responders while completing their daily activities. The NSI is designed to do just that, connect the dots.

Suspicious Activity Report (SAR) Checklist

	Leadership must recognize the importance of implementing a SAR process
	Identify existing SAR processes and determine what SAR processes need to be developed
	Incorporate national guidelines into standard operating procedures
	Implement an agency privacy policy
	Train all agency personnel on the SAR process
	Institutionalize the SAR process within the agency
	Educate the community on the SAR process
	Partner with others and connect to information sharing networks

Situational Awareness Reporting

Fusion centers also should develop a process to manage the reporting to key officials and the public of information regarding significant events (local, regional, national, and international) that may influence state or local security conditions. Fire service constituents should participate in developing and implementing a written policy outlining standard operating procedures to govern the receipt and further dissemination of federally generated information bulletins and situational awareness messages.

If You See Something, Say Something™ **Initiative**

In July 2010, the Department of Homeland Security (DHS), at Secretary Janet Napolitano's direction, launched a national *If You See Something, Say Something*™ public awareness campaign – a simple and effective program to raise public awareness of indicators of terrorism and violent crime. The campaign emphasizes the importance of reporting suspicious activity to the proper state and local law enforcement authorities.

A critical element of the DHS mission is ensuring that the civil rights and civil liberties of persons are not diminished by our security efforts, activities, and programs. Consequently, the *If You See Something, Say Something*™ campaign respects civil rights or civil liberties by emphasizing behavior, rather than appearance, in identifying suspicious activity. Factors such as race, ethnicity, national origin, or religious affiliation alone are not suspicious. For that reason, the public should report only suspicious behavior and situations (e.g., an unattended backpack in a public place or

someone trying to break into a restricted area) rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity. Only reports that document behavior reasonably indicative of criminal activity related to terrorism will be shared with federal partners.

The *If You See Something, Say Something*™ campaign was launched in conjunction with the rollout of the Nationwide Suspicious Activity Reporting Initiative.

Clearances

Only the federal government can grant someone a security clearance. In order to obtain a security clearance, the applicant must work for a government agency or contractor and conduct business that justifies granting him or her access to highly sensitive information. Fire service personnel apply for clearances through DHS, FBI, DOD or DOE depending on the type of mission they are assigned to work on.

What is a Security Clearance?

A security clearance is the process of determining the applicant's trustworthiness and reliability before granting him or her access to national security information.

What is a Security Clearance Investigation?

The Defense Security Service (DSS), the agency that conducts all background and security investigations for the Department of Defense, defines a security clearance investigation as: "A security clearance investigation is an inquiry into an individual's loyalty, character, trustworthiness and reliability to ensure that he or she is eligible for access to national security information. The investigation focuses on an individual's character and conduct, emphasizing such factors as honesty, trustworthiness, reliability, financial responsibility, criminal activity, emotional stability, and other similar and pertinent areas. All investigations consist of checks of national records and credit checks; some investigations also include interviews with individuals who know the candidate for the clearance as well as the candidate himself/herself."[9]

Only federal agencies can provide an individual with a security clearance. They include all national security agencies and intelligence gathering agencies (Central Intelligence Agency, National Security Agency), federal law enforcement agencies (FBI, Secret Service, and Drug Enforcement Administration), civilian military agencies (Defense Intelligence Agency and DSS), certain occupations in the U.S. military, diplomatic agencies (State Department), certain scientific government agencies and a number of others depending on their mission and role in national security.

---

[9] Powers, Rod. "Security Clearance Basics: Part 1, The Basics," http://usmilitary.about.com/cs/generalinfo/a/security.htm.

There are different types of security clearances allowing a person to access classified material. The four main types are confidential, secret, top secret (TS), and sensitive compartmented information (SCI).

Confidential	This type of security clearance provides access to information or material that may cause damage to national security if disclosed without authorization.
Secret	This type of security clearance provides access to information or material that may cause serious damage to national security if disclosed without authorization.
Top Secret (TS)	This type of security clearance provides access to information or material that may cause exceptionally grave damage to national security if disclosed without authorization.
Sensitive Compartmented Information	A SCI clearance is assigned to special compartmented information. A person will only have access to select information relating to that particular compartment, but may not have access to other compartmented information from the same organization.

Fire chiefs may also seek other locally used or employed classifications. One of the most common of these classifications is the Law Enforcement

Sensitive (LES) Classification. This classification is locally applied, but lacks a legislative definition. It is most commonly applied to material that if released could interfere with an ongoing criminal investigation, reveal sources, or compromise investigative procedures. Fire chiefs should discuss with their law enforcement counterparts what this label means in their locality.

Getting Information to the Troops

How to distribute intelligence from Fusion Centers and law enforcement sources to the appropriate level within a fire service organization can become problematic for fire chiefs. The challenges include understanding what intelligence can be passed on and in what manner, how to pass on the intelligence and keep it in the appropriate context, and finally, how to make sure the intelligence is relevant to the local fire department.

Sensitive But Unclassified (SBU) is a designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information (SHSI), Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc.

One way to accomplish this task is to organize your agency around a Fusion Center. The fire chief can partner with the local or state Fusion Center by

providing a full, part time, or additional duty Fusion Liaison Officer to be the primary point of contact with the Fusion Center.

The Fusion Liaison Officer serves as a conduit for facilitating information sharing and product development between the Fusion Center and the fire service. The Fusion Liaison Officer can work with the fusion center to develop briefings for the fire service and deliver those briefings to the appropriate levels of the organization.

There is specialized training available for Fusion Liaison Officers through the Fusion Centers. Depending on the part of the country you are in, Fusion Liaison Officers may also be called Terrorism Liaison Officers or Intelligence Liaison Officers.

Summary

Traditionally, the fire service prides itself on solving its own problems. Fire Chiefs need to be vigilant in solving the problem of not receiving timely intelligence information. They need to be proactive in approaching the appropriate intelligence producers to ensure that their needs and concerns are heard and that they are actively participating in the intelligence process. The training and experience that fire service personnel possess by the nature of their profession make them an excellent resource for contributing to the analysis and production of intelligence on specific incidents. The fire service perspective adds an important dimension to all-hazard risk assessments, preparedness activities and mitigation operations.

These steps are only the first of many that will be required to forge effective terrorism threat intelligence sharing relationships to achieve meaningful

inclusion. To legally and safely handle intelligence—and become a trusted intelligence sharing partner—fire departments will have to develop SOGs, security policies, and privacy policies that meet national standards and protect the reputation of the fire department within the community. Fire departments, out in the community, may be able to prevent terrorism with good intelligence that leads to situational awareness. While this does represent an investment by fire service organizations, the return on that investment is a fire service workforce that is better prepared to effectively and safely manage the evolving terrorism threat.

Online Resources

U.S. Department of Homeland Security Resources
http://www.dhs.gov/files/publications/counterterrorism.shtm

TRIPwire
https://tripwire.dhs.gov

Law Enforcement Online
http://www.fbi.gov/about-us/cjis/leo

Joint Terrorism Task Force and FBI Field Offices
http://www.fbi.gov/contact-us/field

Fusion Center and Intelligence Sharing
http://it.ojp.gov/default.aspx?area=nationallnitiatives&page=1181

Interagency Threat Assessment and Coordination Group
http://www.ise.gov/interagency-threat-assessment-and-coordination-group-itacg