

# INTELLIGENCE ANALYSIS AND PRODUCTION

## Capability Definition

Intelligence Analysis and Production is the merging of data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence with an emphasis on the larger public safety and homeland security threat picture. This process focuses on the consolidation of analytical products among the intelligence analysis units at the Federal, State, local, and tribal levels for tactical, operational, and strategic use. This capability also includes the examination of raw data to identify threat pictures, recognize potentially harmful patterns, or connect suspicious links to discern potential indications or warnings.

## Outcome

Timely, accurate, and actionable intelligence/information products are produced in support of prevention, awareness, deterrence, response, and continuity planning operations.

## Relationship to National Response Plan Emergency Support Function (ESF)/Annex

This capability supports:

Terrorism Incident Law Enforcement and Investigation Incident Annex

## Preparedness Tasks and Measures/Metrics

<b>Activity: Develop and Maintain Plans, Procedures, Programs, and Systems</b>	
<b>Critical Tasks</b>	
Pre.A1c 1.1.1	Provide terminology/lexicon glossary from Federal Government to all relevant fusion center/process entities to eliminate agency-to-agency terminology confusion
Pre.A1c 1.1.2	Use tear-line formats to ensure that State, local and/or tribal officials with varying levels of clearance have access to useful information
Pre.A1c 1.1.3	Develop a broad, national, uniform template for analytic products
PreA1c 1.2	Provide guidance for planners to develop their own current intelligence products, indications and warnings at all levels
PreA1c 1.2.1	Develop guidance for establishing threat at the management level
PreA1c 1.3	Develop means to share regional and State indications and warnings
PreA1c 1.3.1	Develop memoranda of understanding for information sharing with other fusion centers
PreA1c 1.3.2	Develop guidelines for tailoring information according to audience
PreA1c 1.4	Develop plans and procedures for establishing and staffing fusion center
PreA1c 1.4.1	Develop job descriptions and training requirements for personnel

Preparedness Measures	Metrics
A State fusion center strategy is in place that: <ul style="list-style-type: none"> <li>▪ Conforms to <i>Fusion Center Guidelines</i></li> <li>▪ Provides for a coordinated interface to the Federal Government</li> </ul>	Yes/No Yes/No
Fusion center/process participants ensure that analysts understand the tailoring for the different audiences to which they provide information/intelligence	Yes/No
Memorandums of understanding define processes and responsibilities for information sharing and ensure de-confliction with other fusion centers/processes	Yes/No
Appropriate State and local entities provide personnel to the fusion center/process as required	Yes/No
Analysts are granted appropriate clearances by the Department of Homeland Security (DHS)	Yes/No
Job descriptions reflect the region’s applicable risks, threats, and critical infrastructure	Yes/No
Federal standards to pre-qualify the fusion center/process in physical and clearance requirements to receive, store, and control secret/secure information are in place	Yes/No
State and local entities adhere to Federal standards for the fusion center/process in physical and clearance requirements to receive, store, and control secret/secure information	Yes/No
All State, local, and tribal law enforcement information/intelligence databases comply with national standards and are completely compatible for data transmission between pertinent agencies	Yes/No
A clearly defined process to establish threat at the management level, consistent with established intelligence community standards, is in place	Yes/No
A clearly defined process for developing an unclassified briefing is in place	Yes/No
Frequency with which a standardized classified-to-unclassified information review process (including ratio) is conducted	Every 12 months
Unclassified briefings, reports, and alerts are used whenever possible to provide credible information that allows public safety, private-sector, and non-law enforcement agencies to develop intelligence- and information-driven prevention plans without compromising sources or collection methods	Yes/No
Analysts are able to understand and identify links between terrorism-related intelligence and information related to traditional criminal activity so they can identify activities that are indicative of an imminent or potential threat	Yes/No
All personnel demonstrate necessary knowledge of the operating systems and intelligence processes required to perform intelligence functions	Yes/No
Participating agencies have been provided a glossary of terms, updated every 12 months, to the center/process	Yes/No

**Activity: *Develop and Maintain Training and Exercise Programs***

**Critical Tasks**

Pre.A1c 2.1.1	Train permanent and assigned analytical staff on the intelligence cycle and developing analytic products
---------------	--

Pre.A1c 2.1.2	Develop national standard for training fusion center/process staff	
Preparedness Measures		Metric
Each analyst has met a minimum standard for hours of training		Yes/No
Training has met International Association Law Enforcement Analytic Standards from Global Intelligence Working Group and International Association of Law Enforcement Intelligence Analysts (GIWG/IALEIA) based standards (basic, intermediate, advanced)		Yes/No
Percent of personnel trained in the intelligence cycle		100%
Basic and advanced intelligence analysis training is provided for intelligence operations personnel (e.g., commanders/supervisors, officers, analysts)		Yes/No
Percent of fusion center/process staff who receive annual awareness training on relevant privacy and security rules, and regulations (28 CFR and any other relevant State statutes and regulations)		100%
Analysts at relevant agencies and centers/processes are trained to identify precursors and links between crime and terrorism		Yes/No
Analytic staff are properly trained and/or experienced in relevant analytical methods and practices		Yes/No
Percent of analysts at relevant agencies and centers/processes who are trained in the use of analytic methods and tools		100%
Participants have established procedures per the International Association of Law Enforcement Analytic Standards (GIWG/IALEIA) to benchmark analysts' capabilities		Yes/No
Percent of personnel who demonstrate necessary knowledge of the operating systems and intelligence processes required to perform intelligence functions		100%
Analytic staff are knowledgeable in the region's applicable risks, threats, and critical infrastructure		Yes/No
Permanent and assigned analytical staff are trained to meet their responsibilities		Yes/No

**Performance Tasks and Measures/Metrics**

<b>Activity: Establish Fusion Center</b>	
<b>Definition: Establish and operate a multidisciplinary, all-source information/intelligence fusion center/process that undertakes an “all-hazards” and “all-crimes” approach</b>	
Critical Tasks	
Pre.A1c 3.1	Establish and maintain a fusion center/process using the national guidelines and standards; co-locate with an existing entity if practicable/desirable
Pre.A1c 3.2	Sustain technical and procedural connectivity with critical intelligence and information streams
Pre.A1c 3.2.1	Access intelligence and information repositories at all levels of classification as necessary
Pre.A1c 3.2.2	Ensure appropriate technological redundancy
Pre.A1c 3.5	Incorporate the fusion center/process principles of the Criminal Intelligence Model Policy (International Association of Chiefs of Police [IACP])
Pre.A1c 3.3	Establish and maintain communications, including electronic connectivity with other region fusion center/processes

Pre.A1c 3.4	Relay/pass terrorist-related information to the FBI Joint Terrorism Task Force (JTTF) and FBI Field Intelligence Group (FIG)	
Pre.A1c 3.6	Adhere to privacy and security rules in operating fusion center/process	
Performance Measures		Metrics
Key leaders have established and maintained a fusion center/process using the national guidelines and standards per the Global Justice Information Sharing Initiative—Fusion Center Guidelines and Homeland Security Advisory Council (HSAC) recommendations, (Fusion Center Resource CD)		Yes/No
Percent of fusion center staff who have the requisite training and expertise to handle the receipt, analysis, and dissemination of intelligence		100%
The fusion center is appropriately staffed during all operational hours		Yes/No
Information is effectively shared and received using the fusion center technology		Yes/No
The center makes use of the relevant networks, classified and unclassified (e.g., Regional Information Sharing Systems/Law Enforcement Online (RISS/LEO), Homeland Security Information Network (HSIN), and various public health networks)		Yes/No
Access to and from the fusion center/process by those responsible for gathering information is done in accordance with established procedures		Yes/No
Efficient connectivity exists with the Joint Terrorism Task Force (JTTF) and Field Intelligence Guide (FIG))		Yes/No
Staffing of analysts is conducted in accordance with national standards outlined in the Law Enforcement Analytic Standards produced by the Global Intelligence Working Group and International Association of Law Enforcement Intelligence Analysts (GIWG/IALEIA)		Yes/No
The fusion center/process is assigned personnel with diverse subject matter expertise from key departments, organizations, agencies or offices on a permanent, or liaison basis		Yes/No
The fusion center/process received, stored, and controlled secret/secure information		Yes/No
The center/process uses an accessible repository for analytic methods/tools/techniques		Yes/No
A clearly defined process or procedure is used to disseminate information and products		Yes/No

<b>Activity: Access Information</b>	
<b>Definition: Obtain access to and receive collected information associated with the respective territory of the fusion center</b>	
Critical Tasks	
Pre.A1c 4.1	Receive, extract, or collect information from all available sources, including all relevant databases and systems available to the State fusion center, on a continuous basis and with appropriate technological redundancy
Pre.A1c 4.2	Ensure that unclassified briefings, reports and alerts are used whenever possible to provide credible information that allows public safety, private sector and non-law enforcement agencies to develop intelligence- and information-driven prevention plans without compromising source or collection methods

Performance Measures	Metrics
Secret/secure information is received, stored, and controlled in accordance with Federal standards established to prequalify the fusion center/process in physical and clearance requirements	Yes/No
Percent of State, tribal, and local law enforcement databases that are Global Justice XML Data Model (JDXM)-compliant	100%
Unclassified briefings are established using the established process	Yes/No
The standardized classified to unclassified information review process (including ratio) is used	Yes/No
Feedback procedures are followed	Yes/No

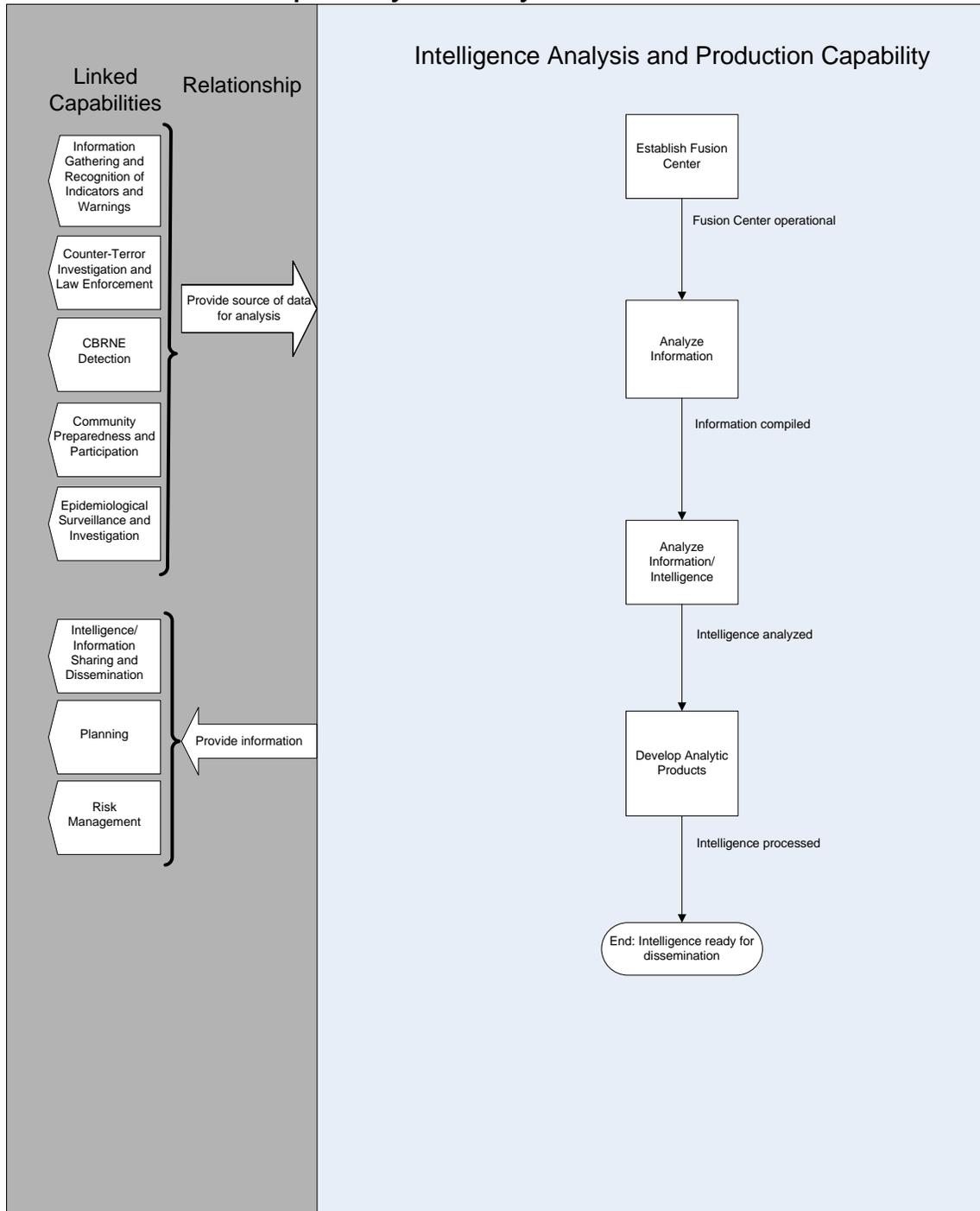
Activity: <i>Analyze Information/Intelligence</i>	
Definition: Integrate and analyze relevant information/intelligence	
Critical Tasks	
Pre.A1c 5.1	Prioritize intelligence based on relevance of the information and the finished intelligence products to potential threat elements
Pre.A1c 5.2.1	Blend, reconcile, and de-conflict data, information, and intelligence received from multiple sources
Pre.A1c 5.2.2	Identify patterns and trends that may indicate emerging, immediate or long-term threat condition
Pre.A1c 5.2.3	Identify links between terrorism related intelligence and information related to traditional criminal activity so as to identify activities indicative of an imminent or potential threat
Pre.A1c 5.2.4	Utilize any and all relevant and useful analytic methodologies, tools, and technology to provide a more comprehensive and useful product
Performance Measures	Metrics
Audit standards are used to review work products	Yes/No
Analysts' capabilities are assessed using procedures per the International Association of Law Enforcement Analytic Standards (GIWG/IALEIA)	Yes/No
Percent of participants who have and use a national template for analytic products provided by Federal authorities	100%
The volume of transactions using information networks are recorded	Yes/No
Actions taken in light of transactions using information networks are tracked	Yes/No

<b>Activity: <i>Develop Analytic Products</i></b>	
<b>Definition: Develop analytic products that are consumer-tailored, clear, and objective and support the development of performance-driven, risk-based prevention, protection, and response programs at all levels</b>	
<b>Critical Tasks</b>	
Pre.A1c 6.1	Provide briefings, reports and/or alerts tailored to recipients with detailed, specific information on actions or activities that may be indicative of an emerging threat
Pre.A1c 6.2	Analyze information needs on a continuous basis for short- and long-term intelligence requirements
Pre.A1c 6.3	Archive information and intelligence in a searchable repository to support future efforts by all fusion analysts
Pre.A1c 6.4	Vet and review products prior to distribution
<b>Performance Measures</b>	
<b>Metrics</b>	
Consumer satisfaction with the analytic product is monitored using an established producer-to-consumer feedback cycle	Yes/No
Analysts tailor requirements for the different audiences to which they provide information/intelligence	Yes/No
The fusion center/process consults the National Criminal Intelligence Sharing Plan and other relevant Federal guidelines for guidance on use of tear-line reports	Yes/No
Percent of products vetted prior to distribution using center/process procedures/mechanisms	100%
Intelligence files are maintained using the standards in the <i>Fusion Center Guidelines</i>	Yes/No
The center/process has an information and intelligence archive	Yes/No
The process used follows the national analytic template in the International Association of Law Enforcement Analytic Standards (GIWG/IALEIA)	Yes/No

***Linked Capabilities***

<b>Linked Capability</b>	<b>Relationship to Capability</b>
Information Gathering and Recognition of Indicators and Warnings	The data collected from Information Gathering and Recognition is further analyzed and processed by Intelligence Analysis and Production
Counter-Terror Investigation and Law Enforcement	Counter-Terror Investigation and Law Enforcement is one source of data analyzed by the Intelligence Analysis and Production capability. The products of the Intelligence Analysis and Production capability may further inform Counter-Terror Investigation and Law Enforcement investigations.
CBRNE Detection	CBRNE Detection is one source of data analyzed by Intelligence Analysis and Production
Community Preparedness and Participation	Citizen reports of suspicious activities is one source of data analyzed by Intelligence Analysis and Production
Epidemiological Surveillance and Investigation	Epidemiological Surveillance and Investigation contributes data for analysis and is provided reports, as appropriate
Intelligence and Information Sharing and Dissemination	The results of the analyses in Intelligence Analysis and Production are disseminated using Intelligence and Information Sharing
Planning	Products that result from Intelligence Analysis and Production are used to ensure that plans adequately address terrorist threats
Risk Management	Products from Intelligence Analysis and Production provide the threat, vulnerability, and consequence data used in risk management

# Capability Activity Process Flow



### Resource Element Description

Resource Elements	Components and Description
Fusion Center/process	A multidisciplinary, all-source information/intelligence fusion center/process that undertakes an “all hazards” and “all crises” approach
Multi-discipline Analysts	Analyst personnel for multiple disciplines (e.g., public health, HazMat, etc.) to support intelligence analysis
Intelligence personnel	Personnel involved in intelligence analysis at various levels within the organization (e.g. analysts, supervisors, officers, etc.)
Administrative and support personnel	Personnel who perform administrative and support functions (e.g., information technology/communications, fusion center staff, security, etc.)
Public Health Analysts	Federal, regional, State, local, tribal, and other appropriate agency public health personnel involved in intelligence analysis
Cleared personnel	Personnel possessing valid and current security clearances
Joint Terrorism Task Forces (JTTFs)	Task forces formed at the local level and composed of persons from various government and private elements (e.g., law enforcement, public health, local businesses, key infrastructure representatives, emergency management and other first responders)
Hardware, software, and internet-based systems	Hardware, software, and internet-based systems that allow for information exchange and dissemination
Terminals with access to information sharing networks and early detection/alert programs and networks	Information sharing network architecture (e.g., Regional Information Sharing System (RISS)/Law Enforcement Online (LEO), Joint Regional Exchange System (JRIES), National Law Enforcement Telecommunication System (NLETS), FBI Criminal Justice Information Services/National Crime Information Center (CJIS/NCIC) networks).  Access to early detection/alert programs and networks and all-source information (i.e., Public Health Information Network, Biosense, Homeland Security Information Network, Information Sharing and Analysis Centers, etc.). Relevant systems include: RSS/LEO, HSIN, etc.
Intelligence analysis and maintenance tools	Software and equipment to include surveillance systems/equipment, recording systems/equipment analyzing software/systems, data synthesis software, data storage
Data synthesis software	Hazard prediction, assessment, and threat modeling software

### Planning Assumptions

- Prevention consists of those activities that serve to detect, deter, and disrupt terrorist threats or actions against the United States and its interests. These activities decrease the perpetrators’ chance of success, mitigate attack impact, minimize attack visibility, increase the chance of apprehension or detection, and obstruct perpetrators’ access to resources. Tasks in this area are important regardless of a single type of threat, adversary capability, time or location of incident. Similarly, these capabilities reflect many tasks routinely undertaken by law enforcement and related organizations as they conduct traditional all-hazards, all-crimes activities.
- This capability applies to all potential terrorist incidents and is applicable to all 12 terrorism-related National Planning Scenarios. The analysis of national targets focused on bombing using improvised explosives device, chlorine tank explosion, aerosol anthrax, improvised nuclear device, and a radiological dispersal.

- Effective prevention depends on timely, accurate, and actionable information about the adversary, their operations, their support, potential targets, and methods of attack. Homeland security intelligence/information fusion is the overarching process of managing the development and flow of information and intelligence across all levels and sectors of government and the private sector on a continual basis. Although the primary emphasis of fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to Federal, State, local, and tribal entities is that it will support ongoing efforts to address non-terrorism-related, all-hazards, all-crimes issues.
- The Planning Factors for A Single Incident section and the Approaches for Large-Scale Events section do not apply because there is no incident or large-scale event that necessarily occurs before these capabilities come in to play.
- Intelligence/information fusion is an ongoing, cyclical process that incorporates three primary capabilities: Information Gathering and Recognition of Indicators and Warnings; Intelligence Analysis and Production; and Intelligence and Information Sharing and Dissemination.
- All appropriate objectives and critical tasks will be exercised regularly at all levels in order to measure performance and demonstrate capability.

***Planning Factors for a Single Incident***

Not Applicable

***Approaches for Large-Scale Events***

Not Applicable

***Target Capability Preparedness Level***

Resource Element Unit	Type of Element	Number of Units	Unit Measure (number per x)	Lead	Capability Activity supported by Element
Fusion Centers/process	Personnel	1	Per jurisdiction/region	Federal, State, Local (Intrastate region, City)	Establish Fusion Center Analyze Information Analyze Information/Intelligence Develop Analytic Products
Multi-discipline Analysts	Personnel	As Needed	Provided from appropriate agencies on a permanent or liaison basis	Federal/State/Local	All Activities
Intelligence personnel	Personnel	As Needed	Provided from law enforcement agencies on a permanent or liaison basis	Federal/State/Local	All Activities

Resource Element Unit	Type of Element	Number of Units	Unit Measure (number per x)	Lead	Capability Activity supported by Element
Administrative and support personnel	Personnel	As Needed	Provided from appropriate agencies on a permanent or liaison basis	Federal/State/Local	All Activities
Public Health Analysts	Personnel	As Needed	Provided from public health agencies on a permanent or liaison basis	Federal/State/Local	All Activities
Cleared personnel	Personnel	As Needed		Federal/State/Local	All Activities
Joint Terrorism Task Forces (JTTFs)	Personnel	As Needed		Federal/State/Local	All Activities
Hardware, software, and internet-based systems that allow for information exchange and dissemination	Systems	As Needed		Federal/State/Local	All Activities
Terminals with access to information sharing networks and early detection/alert programs and networks	Equipment	As Needed	Per fusion center site	Federal/State/Local	All Activities
Intelligence analysis and maintenance tools	Systems	As Needed	Per fusion center site	Federal/State/Local	All Activities
Data synthesis software	Equipment	As Needed		Federal/State/Local	All Activities

**References**

1. Homeland Security Presidential Directive/HSPD-8: National Preparedness. December 2003. <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html>.
2. National Response Plan. U.S. Department of Homeland Security. December 2004.
3. National Incident Management System. U.S. Department of Homeland Security. March 2004. <http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf>.

4. The Office for Domestic Preparedness Guidelines for Homeland Security: Prevention and Deterrence. U.S. Department of Homeland Security, Office for Domestic Preparedness. June 2003. <http://www.ojp.usdoj.gov/odp/docs/ODPPrev1.pdf>.
5. Information/Intelligence Sharing System Survey. Global Intelligence Working Group. 2001. [http://it.ojp.gov/documents/intell\\_sharing\\_system\\_survey.pdf](http://it.ojp.gov/documents/intell_sharing_system_survey.pdf).
6. Fusion Center Guidelines. Global Justice Information Sharing Initiative. July 2005.
7. The National Criminal Intelligence Sharing Plan. U.S. Department of Justice, Global Justice Information Sharing Initiative. 2004. [http://it.ojp.gov/documents/National\\_Criminal\\_Intelligence\\_Sharing\\_Plan.pdf](http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf).
8. Law Enforcement Analytic Standards. Global Justice Information Sharing Initiative and International Association of Law Enforcement Intelligence Analysts, Inc. November 2004.
9. Applying Security Practices to Justice Information Sharing, Version 2. U.S. Department of Justice, Global Justice Information Sharing Initiative, Security Working Group. March 2004. [http://it.ojp.gov/documents/200404\\_ApplyingSecurityPractices\\_v\\_2.0.pdf](http://it.ojp.gov/documents/200404_ApplyingSecurityPractices_v_2.0.pdf).
10. Central Intelligence Agency (CIA) Fact Book on Intelligence.
11. Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues. GAO-03-1165T. U.S. General Accounting Office. September 2003. <http://www.gao.gov/new.items/d03715t.pdf>.
12. Doctrine for Intelligence Support to Joint Operations. Joint Publication 2-0. Joint Chiefs of Staff, Director of Intelligence. March 2000. [http://www.fas.org/irp/doddir/dod/jp2\\_0.pdf](http://www.fas.org/irp/doddir/dod/jp2_0.pdf).
13. The 9/11 Commission Report. National Commission on Terrorist Attacks upon the United States. July 2004. <http://www.9-11commission.gov/>
14. Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq. Select Committee on Intelligence, U.S. Senate, 108th Congress. July 2004. <http://intelligence.senate.gov/iraqreport2.pdf>.
15. The Homeland Security Advisory Council Prevention and Information Sharing Working Group. 2004.
16. Fusion Center Initiative. Homeland Security Advisory Council. April 2005.
17. State, Tribal and Local Intelligence and Information Sharing Initiative. Homeland Security Advisory Council. December 2004.
18. Private Sector Information Sharing Initiative. Homeland Security Advisory Council. June 2005.
19. National Strategy for Homeland Security. Office of Homeland Security. July 2002. [http://www.whitehouse.gov/homeland/book/nat\\_strat\\_hls.pdf](http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf).
20. Presidential Directive-39: U.S. Policy on Counterterrorism. June 21, 1995. <http://www.ojp.usdoj.gov/odp/docs/pdd39.htm>.
21. Presidential Directive-62/63: Protection Against Unconventional Threats to the Homeland and Americans Overseas. Critical Infrastructure Protection, National Plan for Information Systems Protection. May 22, 1998. <http://www.fas.org/irp/offdocs/pdd-63.htm>