

# INFORMATION GATHERING AND RECOGNITION OF INDICATORS AND WARNINGS

## Capability Definition

The Information Gathering and Recognition of Indicators and Warning Capability entails the gathering, consolidation, and retention of raw data and information from sources to include human sources, observation, technical sources and open (unclassified) materials. Unlike intelligence collection, information gathering is the continual gathering of only pure, unexamined data, not the targeted collection traditionally conducted by the intelligence community or targeted investigations. Recognition of indicators and warnings is the ability to see in this gathered data the potential trends, indications, and/or warnings of criminal and/or terrorist activities (including planning and surveillance) against U.S. citizens, government entities, critical infrastructure, and/or our allies.

## Outcome

Locally generated threat and other criminal and/or terrorism-related information is identified, gathered, entered into an appropriate data/retrieval system, and provided to appropriate analysis centers.

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

This capability supports:

Terrorism Incident Law Enforcement and Investigation Annex

## Preparedness Tasks and Measures/Metrics

Activity: <i>Develop and Maintain Plans, Procedures, Programs, and Systems</i>	
Critical Tasks	
Pre.A1b 1.1	Develop and maintain operationally sound policies to comply with regulatory, statutory, privacy, and other issues that may govern the gathering of information
Pre.A1b 1.2	Develop and maintain procedures, systems, and/or technology to process the inflow of gathered information from all sources in a timely fashion
Pre.A1b 1.3	Develop and provide States and tribal authorities with information needs clearly defined by the Federal community based on the threat environment in a timely manner
Pre.A1b 1.4	Provide the Federal community with feedback on specificity and relevance of Federal information needs products defined by the State
Pre.A1b 1.5	Communicate information needs from Federal community and States to local law enforcement, Tribal, private-sector, and other appropriate personnel as needed and in a timely manner
Pre.A1b 1.6	Provide feedback from information-gathering entities to the State on specificity and relevance of State information needs products

Pre.A1b 1.7	Develop and communicate baseline indicators and warnings sets from Federal community to State and Tribal authorities	
Pre.A1b 1.8	Determine within the Federal community Essential Elements of Information (EEI) that can be used to identify terrorist operations	
<b>Preparedness Measures</b>		<b>Metrics</b>
State, tribal, and local areas have a clearly defined, implemented, and audited process in their jurisdiction for requesting information from the Federal community, generally through their State’s designated senior official	Yes/No	
Key stakeholders in the Federal community have developed clear and concise information needs based on the threat environment	Yes/No	
The Federal community has delivered its information needs to each State’s designated senior officials using a clearly defined process	Yes/No	
Each State’s designated senior officials can verify receipt of information needs from the Federal community (or demonstrate an understanding of information needs)	Yes/No	
Frequency with which Federal community updates its information needs	Every 12 months	
Information needs products contain a feedback mechanism	Yes/No	
Processes by which State, tribal, and/or local authorities request information from the Federal community is in place	Yes/No	
Process by which the State uniformly and consistently communicates information needs to the local level is in place	Yes/No	
Regulatory, statutory, and/or privacy policies that govern the gathering of information are in place	Yes/No	
A clearly defined process for passing information gathered by law enforcement and other agencies during routine day-to-day activities into the information-sharing network is in place	Yes/No	
Feedback is provided to those responsible for gathering information during routine day-to-day activities	Yes/No	
The process for passing information gathered by law enforcement and other agencies has been audited	Yes/No	
Law enforcement and appropriate agencies are have audited plans, processes, and technology in place that enable them to do the following: <ul style="list-style-type: none"> <li>▪ Identify items and materials used by criminal and/or terrorist organizations and report suspicious activities related to them</li> <li>▪ Gather information on critical infrastructure and other potentially high-risk locations and assets</li> <li>▪ Increase information gathering activities regarding critical infrastructure and other potentially high-risk locations and assets, during an elevated threat level</li> <li>▪ Coordinate information gathering operations across jurisdictions</li> <li>▪ Process gathered information</li> <li>▪ Provide all operational personnel with the most recent indicators and warnings to report</li> </ul>	Yes/No Yes/No Yes/No Yes/No Yes/No Yes/No	
Percent of jurisdictions that have an established system for public reporting of suspicious activity (e.g., 911, tip lines)	100%	

Appropriate governmental entities operate or participate in public education programs to raise public awareness of suspicious activities and how to report them	Yes/No
Content and template standards for reported information are in place	Yes/No
Processes, protocols, and technical capabilities to allow extraction of information from public, private, and law enforcement databases are in place	Yes/No

<b>Activity: <i>Develop and Maintain Training and Exercise Programs</i></b>	
<b>Critical Tasks</b>	
Pre.A1b 2.1.1	Develop and initiate terrorism indicator sets and relationships training programs
Pre.A1b 2.1.2	Develop and distribute information gathering and reporting programs
Pre.A1b 2.1.6	Develop and initiate critical infrastructure surveillance technique and criteria
Pre.A1b 2.1.4	Provide training feedback to Federal trainers
<b>Preparedness Measures</b>	<b>Metrics</b>
Law enforcement and public safety personnel who shall be trained in information gathering and recognition of indicators and warnings have been identified.	Yes/No
The following training has been provided to identified personnel: <ul style="list-style-type: none"> <li>▪ Training in recognizing criminal and/or terrorism indicators and warnings</li> <li>▪ Refresher training in indicators and warnings</li> <li>▪ Training in critical infrastructure (CI) surveillance</li> <li>▪ Advanced training programs</li> </ul>	Yes/No Yes/No Yes/No Yes/No
Federally developed training in recognizing and reporting indicators and warnings at identified businesses (via a train-the-trainer program) is conducted	Yes/No
Businesses in each jurisdiction that should be targeted for training in indications and warnings have been identified	Yes/No
Frequency with which government training entities review and update training materials	Every 12 months
Government training entities conduct Federally developed training in recognizing indicators and warnings to appropriate State, tribal, and local entities	Yes/No

**Performance Tasks and Measures/Metrics**

<b>Activity: <i>Gather Information</i></b>	
<b>Definition: Gather information that could be used to identify terrorist operations from all sources (e.g., law enforcement, public health, public works, transportation, firefighting and emergency medical entities) through routine activities</b>	
<b>Critical Tasks</b>	
Pre.A1b 3.1	Gather homeland security information during routine day-to-day activities and pass to appropriate authorities
Pre.A1b 3.1.1	Identify items and materials used by criminal and/or terrorist organizations to carry out attacks

Pre.A1b 3.1.2	Catalog information provided by all sources and retain in a database to enable timely retrieval	
Pre.A1b 3.2	Conduct information gathering operations on critical infrastructure and other potentially high-risk locations or assets	
Pre.A1b 3.3	Coordinate information gathering activities with relevant local, tribal, State, and Federal entities on an ongoing basis, in particular with the Joint Terrorism Task Force (JTTF) in terrorism-related cases	
Pre.A1b 3.3.1	Establish short, medium, and long term coordinated information gathering policies, procedures and systems	
Performance Measures		Metrics
Information was organized, linked, searchable, and easily retrievable		Yes/No
Information provided by all sources met predefined standards for accuracy, completeness and consistency		Yes/No
The process for passing information gathered during routing activities was implemented		Yes/No
Information was passed to appropriate authorities using a clearly defined process, utilizing predefined network channels		Yes/No
The effectiveness of this process was assessed by appropriate agencies		Yes/No
Feedback was provided to those responsible for gathering information		Yes/No

**Activity: *Identify Suspicious Circumstances***

**Definition: Recognize and identify suspicious circumstances or indicators and warnings associated with planning, support, and operations related to potential criminal and/or terrorist-related activities**

**Critical Tasks**

Pre.A1b 4.1	Recognize suspicious activities involving items and materials used by criminal and/or terrorist organizations
Pre.A1b 4.2	Recognize and identify suspicious circumstances or indicators and warnings that may be associated with planning, support, and operations related to potential criminal and/or terrorist-related activities
Pre.A1b 4.3	Utilize a predefined notification process to advise law enforcement of suspicious activity
Pre.A1b 4.4	Notify law enforcement of potential terrorist activities in/around or related to private sector businesses/operations

Performance Measures		Metrics
Law enforcement personnel followed-up with a reporting organization if more information was necessary		Yes/No
Law enforcement personnel acted on authenticated information		Yes/No
Law enforcement personnel used approved response protocols to dispatch the appropriate public or private sector personnel to the potential threat		Yes/No
Upon examination at the incident scene, law enforcement or related personnel were able to differentiate suspicious behaviors and activities from illegal or potentially threatening actions		Yes/No

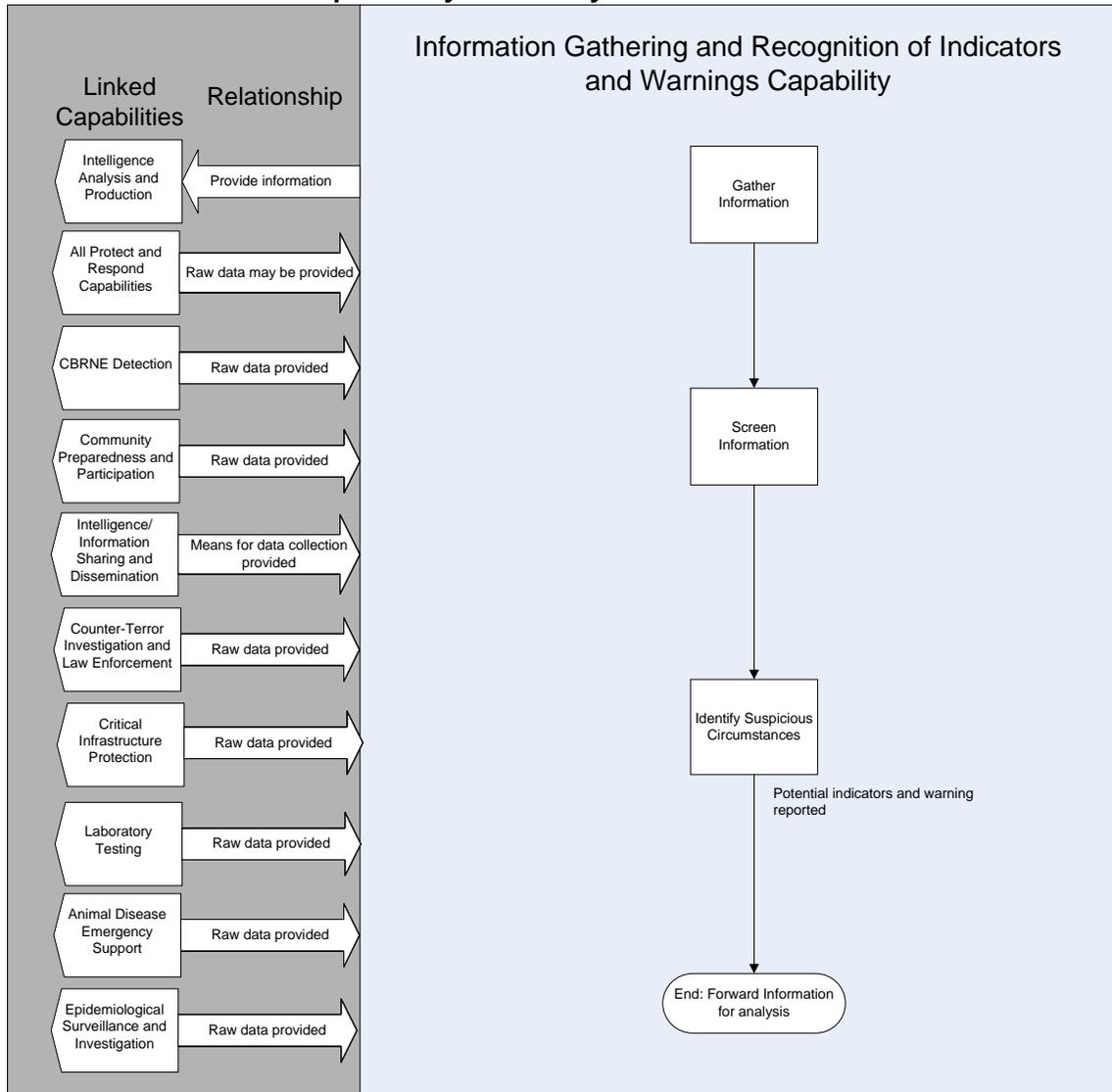
Key private-sector businesses used an established communication avenue to report suspicious activities to appropriate Federal, State, local, or tribal law enforcement entities	Yes/No
The general public has been advised how to recognize suspicious activity (e.g., 911 tip lines, etc.)	Yes/No
The general public was familiar with and used a predefined notification process to advise law enforcement of suspicious activity	Yes/No

<b>Activity: Screen Information</b>	
<b>Definition: Receive, authenticate, and screen information for relevance, with the appropriate level of oversight/supervision and in a timely manner</b>	
<b>Critical Tasks</b>	
Pre.A1b 5.1	Provide guidance to create linked, compatible national database architecture
Pre.A1b 5.2	Query databases or records to check for significance of information
Pre.A1b 5.3	Maintain and update procedures and/or systems to process the inflow of gathered information from all sources in a timely fashion
<b>Performance Measures</b>	
	<b>Metrics</b>
Relevant personnel had access to systems or technology in order to enter gathered information	Yes/No
Database systems were linked and compatible allowing for rapid transmission and processing of pertinent information	Yes/No
Gathered information was processed using clearly defined procedures	Yes/No
Information was traceable, allowing for easy communication between disseminator and analyst	Yes/No
Procedures for tracking information were audited	Yes/No
All pertinent information was cataloged and databased to enable timely retrieval	Yes/No
Intelligence related to high risk infrastructure or an acute threat was prioritized and reported as soon as it was observed	Yes/No
Information provided by all sources was corroborated	Yes/No
Information was catalogued and files are maintained in accordance with standards in the <i>Fusion Center Guidelines</i>	Yes/No
Information was extracted in accordance with approved processes, protocols, and technical capabilities	Yes/No

**Linked Capabilities**

Linked Capability	Relationship to Capability
Animal Disease Emergency Support	Animal Disease Emergency Support monitoring activities may provide a source of data for Information Gathering
CBRNE Detection	Data from detection devices/processes may be a source of data for Information Gathering
Community Preparedness and Participation	Information provided by citizens via hot lines and other collection centers may be a source of data for Information Gathering
Food and Agricultural Safety and Defense	Food and Agricultural monitoring activities may provide a source of data for Information Gathering
Intelligence Analysis and Production	Information Gathering provides the data used by Intelligence Analysis and Production
Intelligence and Information Sharing and Dissemination	Intelligence and Information Sharing provides the means for collecting the data from various sources
Counter-Terror Investigation and Law Enforcement	Data gathered through Counter-Terror Investigation and Law Enforcement may provide a source of data for Information Gathering
Laboratory Testing	Laboratory analysis may provide a source of data for Information Gathering
Epidemiological Surveillance and Investigation	Epidemiological surveillance may provide a source of data for Information Gathering
Critical Infrastructure Protection	Critical Infrastructure Protection is a source of data for Information Gathering

## Capability Activity Process Flow



**Resource Element Description**

Resource Elements	Components and Description
Information gathering personnel	Multi-agency/discipline personnel at all levels to support information identification, gathering, and recognition (e.g., medical personnel, law enforcement, etc.)
Information processing personnel	Personnel at all levels to process (receive, authenticate, and screen) information
Joint Terrorism Task Force (JTTF)	Task forces formed at the local level and composed of persons from various government and private entities (e.g., law enforcement, public health, local businesses, key infrastructure representatives, emergency management and other first responders)
Public reporting system	System for public reporting of suspicious activity (911, tip lines, etc.)
Information gathering systems and equipment	Surveillance and detection systems/equipment, data gathering and analyzing systems (dedicated software), access to early detection/alert programs and networks, and all-source information

**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. Initial planning, however, has been focused on bombings 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.
- 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.
- Both the Planning Factors for a Single Incident section and the Approaches for Large-Scale Events section have been omitted because there is no incident or large-scale event that necessarily occurs before these capabilities come in to play.

**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
Information gathering personnel	Personnel	As Needed		Federal/State/Local/Private Sector	Gather Information Screen Information Identify Suspicious Circumstances
Information processing personnel	Personnel	As Needed		Federal/State/Local	Gather Information Screen Information Identify Suspicious Circumstances
Joint Terrorism Task Force (JTTF)	Federal Resource Organization	As Needed		Federal	Gather Information Screen Information Identify Suspicious Circumstances
Public reporting system	Equipment	As Needed		Federal/State/Local	Gather Information Screen Information Identify Suspicious Circumstances
Information Gathering Systems and Equipment	Equipment	As Needed		Federal/State/Local/Private Sector	Gather Information Screen Information Identify Suspicious Circumstances

**References**

1. 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>.
2. Homeland Security Presidential Directive/HSPD-8: National Preparedness. December 2003. <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html>.
3. National Response Plan. U.S. Department of Homeland Security. December 2004.
4. National Incident Management System. U.S. Department of Homeland Security. March 2004. <http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf>.
5. U.S. Department of Homeland Security Priority Information Requirements. July 2004–January 2005.

6. 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).
7. Fusion Center Guidelines. Global Justice Information Sharing Initiative. July 2005.
8. The National Criminal Intelligence Sharing Plan. Global Justice Information Sharing Initiative, U.S. Department of Justice. Revised June 2005. [http://it.ojp.gov/documents/National\\_Criminal\\_Intelligence\\_Sharing\\_Plan.pdf](http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf).
9. Fusion Center Initiative. Homeland Security Advisory Council. April 2005.
10. State, Tribal, and Local Intelligence and Information Sharing Initiative. Homeland Security Advisory Council. December 2004.
11. Private Sector Information Sharing Initiative. Homeland Security Advisory Council. June 2005.
12. Homeland Security Information Network. <http://www.dhs.gov/dhspublic/display?theme=43&content=3747&print=true>.
13. 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>.
14. 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).
15. 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).
16. 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).
17. 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>.
18. The 9/11 Commission Report. National Commission on Terrorist Attacks upon the United States. July 2004. <http://www.9-11commission.gov/>.