INTELLIGENCE AND INFORMATION SHARING AND DISSEMINATION

Capability Description

The Intelligence and Information Sharing and Dissemination capability provides necessary tools to enable efficient prevention, protection, response, and recovery activities. Intelligence/ Information Sharing and Dissemination is the multi-jurisdictional, multidisciplinary exchange and dissemination of information and intelligence among the Federal, State, local, and tribal layers of government, the private sector, and citizens. The goal of sharing and dissemination is to facilitate the distribution of relevant, actionable, timely, and preferably declassified or unclassified information and/or intelligence that is updated frequently to the consumers who need it. More simply, the goal is to get the right information to the right people at the right time.

An effective intelligence/information sharing and dissemination system will provide durable, reliable, and effective information exchanges (both horizontally and vertically) between those responsible for gathering information and the analysts and consumers of threat-related information. It will also allow for feedback and other necessary communications in addition to the regular flow of information and intelligence.

Outcome

Effective and timely sharing of information and intelligence occurs across Federal, State, local, tribal, territorial, regional, and private sector entities to achieve coordinated awareness of, prevention of, protection against, and response to a threatened or actual domestic terrorist attack, major disaster, or other emergency.

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

This capability supports the following Emergency Support Functions (ESFs)/Annexes:

ESF #1: Transportation
ESF #2: Communications
ESF #3: Public Works and Engineering
ESF #4: Firefighting
ESF #5: Emergency Management
ESF #6: Mass Care, Housing, and Human Services
ESF #7: Resource Support
ESF #8: Public Health and Medical Services
ESF #9: Urban Search and Rescue
ESF #10: Oil and Hazardous Materials Response
ESF #11: Agriculture and Natural Resources
ESF #12: Energy
ESF #13: Public Safety and Security
ESF #14: Long-Term Recovery and Mitigation
Biological Incident Annex

`

Cyber Incident Annex
Terrorism Incident Law Enforcement and Investigation Annex

Preparedness Tasks and Measures/Metrics

Activity: ***Develop and Maintain Plans, Procedures, Programs, and Systems***	
Critical Tasks	
ComG 1.1.1	Identify all Federal, State, regional, tribal, and local stakeholders for inclusion in the information sharing framework
ComG 1.1.2	Identify non-law enforcement governmental entities and officials for inclusion in the information sharing framework
ComG 1.1.3	Identify appropriate law enforcement and other enforcement governmental personnel for receipt of security clearances at an appropriate level to ensure effective dissemination of critical information
ComG 1.2.1	Develop information sharing network standards: survivable, interoperable, compatible, secure, accessible
ComG 1.2.2	Develop alternate, supplemental, and back-up routing procedures
ComG 1.3	Develop and maintain operationally sound policies to comply with regulatory, statutory, privacy, and other issues that may govern the gathering of information
ComG 1.4	Develop regulatory, statutory, and/or privacy policies
ComG 1.4.1	Develop a clearly defined process for preventing, reporting, and addressing the inappropriate disclosure of information and/or intelligence
ComG 1.4.2	Develop a clearly defined mechanism/process (reduced to a single pipeline wherever possible or prudent) for sharing information/intelligence between Federal and State sources
ComG 1.4.3	Establish alternative, supplemental, and back-up mechanisms for routing information and/or intelligence to the necessary agencies

Preparedness Measures	**Metrics**
Frequency with which informational distribution lists with points of contact are updated	Every month
Relevant Federal, State, regional, local, and tribal authorities have been identified as necessary participants in the information sharing process	Yes/No
Relevant Federal, State, regional, local, and tribal authorities have access to the necessary information sharing systems	Yes/No
Memoranda of understanding (MOU) or similar agreements between appropriate entities are in place	Yes/No
Federal agencies have a process in place to declassify or provide tear lines for relevant information and/or intelligence	Yes/No
The number of law enforcement and other governmental personnel identified to receive security clearances meets jurisdictional requirements/needs	Yes/No
Appropriate Federal, State, regional, local, and tribal law enforcement and other	Yes/No

governmental personnel receive security clearances at an appropriate level of classification	
Regulatory, statutory, and/or privacy policies are in place	Yes/No
Federal, State, regional, local, and tribal law enforcement entities have a clearly defined, implemented, and audited process for preventing, reporting, and addressing the inappropriate disclosure of information and/or intelligence	Yes/No
Clearly defined and documented mechanisms/processes (reduced to a single pipeline wherever possible and prudent) for sharing information/intelligence among Federal, State, regional, local, and tribal sources are in place	Yes/No
Mechanisms/processes for sharing information/intelligence among Federal, State, regional, local, and tribal sources are technologically proficient for the entities involved	Yes/No
Alternative, supplemental, and back-up mechanisms for routing information and/or intelligence to the necessary agencies are available and routinely evaluated	Yes/No
Mechanisms within the information sharing network to provide feedback and/or follow-up information as needed are in place	Yes/No
Local agencies have an established procedure/protocol for providing intelligence products or relevant information to street-level law enforcement personnel	Yes/No
Fusion Centers/processes ensure the participation of appropriate private-sector entities	Yes/No
The Department of Homeland Security (DHS) Information Sharing and Analysis Center (ISAC) program ensures the participation of appropriate private-sector entities	Yes/No
Joint Terrorism Task Forces have a process for sharing relevant information with the private sector in a timely manner	Yes/No
Access to early detection/alert programs and networks and all-source information is available (e.g., Public Health Information Network, BioSense, Homeland Security Information Network, Information Sharing and Analysis Centers, etc.) as appropriate	Yes/No

Activity: *Develop and Maintain Training and Exercise Programs*	
Critical Tasks	
ComG 2.2.1	Design and conduct exercises to test Intelligence and Information Sharing and Dissemination tasks within a single unit and jointly with other jurisdictions and levels of government
ComG 2.1.1	Train appropriate personnel on intelligence/information sharing and disseminate processes and procedures

Preparedness Measures	**Metrics**
There are adequate numbers of trained personnel at all levels (especially at dispatch or communications centers) to process and disseminate information	Yes/No
Personnel are aware of and trained to adhere to pre-defined security clearances and need-to-know parameters	Yes/No
Appropriate personnel are trained in processing and disseminating information and intelligence	Yes/No
Personnel are trained in the process for preventing, reporting, and addressing the inappropriate disclosure of information and/or intelligence	Yes/No

`

Exercises test the process for preventing, reporting, and addressing the inappropriate disclosure of information and/or intelligence	Yes/No
All appropriate law enforcement personnel have received the Criminal Intelligence Coordinating Council (CICC) Outreach Package	Yes/No
All appropriate law enforcement personnel promote the concept of intelligence-led policing as outlined in the CICC Outreach Package	Yes/No
Training and exercise programs include interaction with the private sector operators of critical infrastructure	Yes/No
Exercises test alternative, supplemental, and back-up mechanisms for routing information and/or intelligence to the necessary agencies	Yes/No

Performance Tasks and Measures/Metrics

Activity: *Incorporate All Stakeholders in Information Flow*	
Definition: Identify and share information with all pertinent stakeholders across all disciplines through a clearly defined information sharing system	
Critical Tasks	
ComG 3.1	Share information and/or intelligence between Federal, State, local, and tribal levels by using clearly defined mechanisms/processes
ComG 3.1.1	Adhere to predefined security clearances and need-to-know parameters when disseminating information and intelligence
ComG 3.1.2	Comply with regulatory, statutory, privacy-related, and other issues that may govern the sharing of information
ComG 3.1.3	Prevent, report, and/or address inappropriate disclosures of information and/or intelligence

Performance Measures	**Metrics**
Compliance with regulatory, statutory, privacy-related, and other issues that govern the sharing of information is audited on a regular basis	Yes/No
Percent of inappropriate disclosures of information and/or intelligence for which records are maintained	100%
Percent of inappropriate disclosures of information and/or intelligence that are reported and resolved according to established processes	100%

Activity: *Vertically Flow Information*	
Definition: Share information vertically (up and down from the Federal level) within law enforcement and other appropriate agencies in a timely and effective manner	
Critical Tasks	
ComG 4.1	Share intelligence and information systematically between Federal, State, local, and regional entities in a timely manner

ComG 4.1.1	Disseminate relevant intelligence and/or information from Federal or State entities to local authorities in a usable format and in a timely manner
ComG 4.1.3	Disseminate relevant information and/or intelligence products to street-level law enforcement personnel
ComG 4.1.2	Provide relevant intelligence and/or information from local authorities to Federal or State entities in a usable format and in a timely manner
ComG 4.2.2	Declassify or provide tear lines for relevant information and/or intelligence

Performance Measures	**Metrics**
Time in which relevant information received from the fusion center is disseminated to street-level personnel	Within 12 hours from receipt at the fusion center
Percent of law enforcement intelligence/information passed to local authorities that is deemed useful or actionable	100%

Activity: ***Horizontally Flow Information***

Definition: Share information across disciplines (among fire departments, EMS units, public works, the private sector, and so forth) at all levels and across jurisdictions in a timely and efficient manner

Critical Tasks	
ComG 5.1	Adhere to horizontal coordination across jurisdictions among law enforcement and other appropriate agencies at all levels through effective and timely information sharing
ComG 5.1.1	Share intelligence and/or information across disciplines in a timely and effective manner
ComG 5.2	Structure dissemination and information sharing mechanisms so that private-sector entities receive accurate, timely, and unclassified information that is updated frequently and is consistent with their formal intelligence requirements

Performance Measures	**Metrics**
A clearly defined process or procedure is used to disseminate information and products	Yes/No
Intelligence and/or information is shared across disciplines in a timely manner	Yes/No

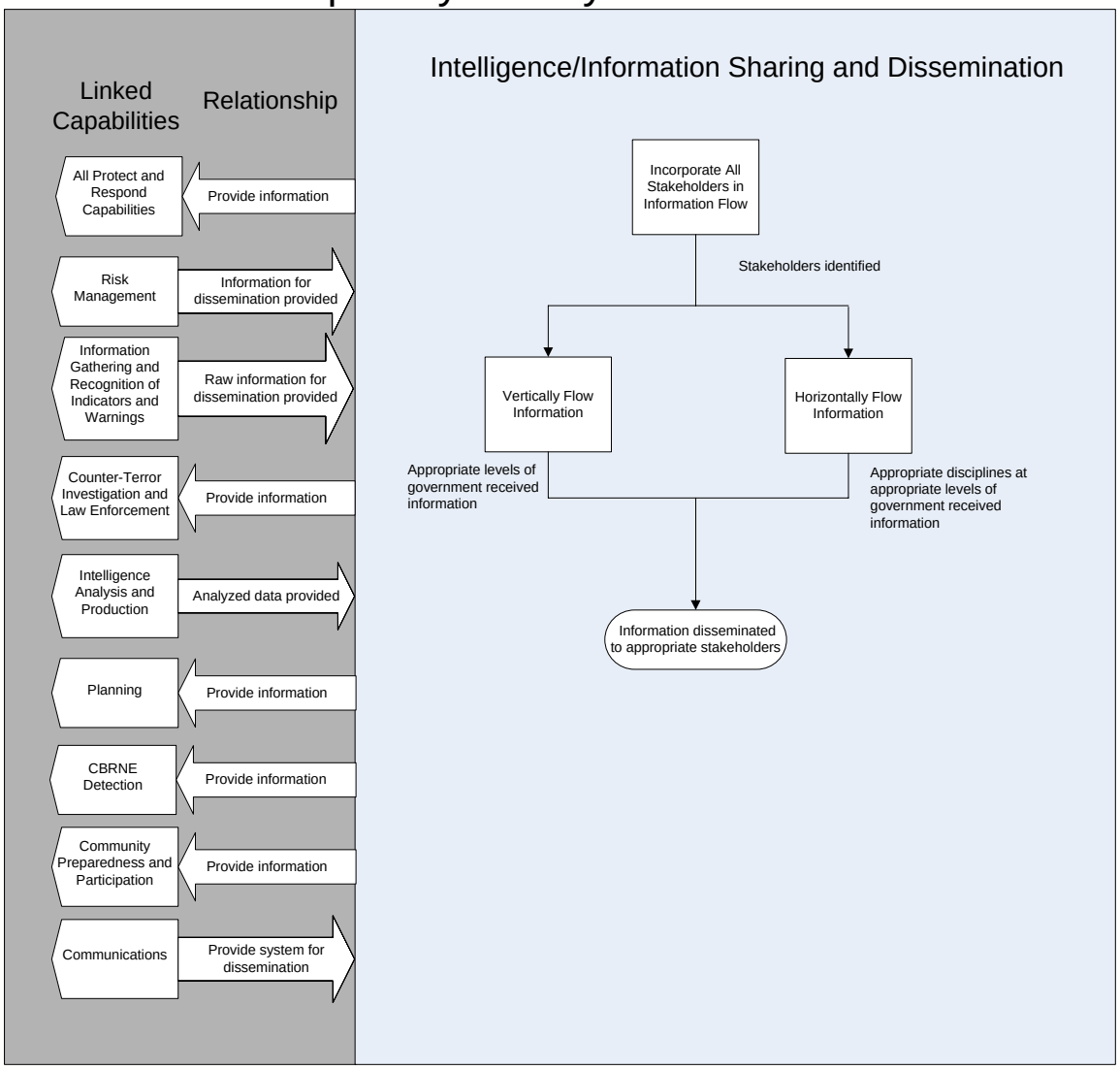
Linked Capabilities

Linked Capability	Relationship to Capability
All Protect Capabilities	Intelligence and Information Sharing and Dissemination provides the means for sharing data on suspected and actual threats, which prompts additional monitoring and the implementation of specific protection activities. Monitoring results from the Protect Capabilities is further shared as needed through this Capability.
All Respond Capabilities	Intelligence and Information Sharing and Dissemination provides the means for sharing data needed to carry out response activities effectively. Results of response actions are then further shared as needed through this Capability.

`

Linked Capability	Relationship to Capability
Risk Management	Intelligence and Information Sharing and Dissemination provides the means for sharing threat, vulnerability, and consequence data used in risk management.
Information Gathering and Recognition of Indicators and Warnings	The data gathered through Information Gathering & Recognition is communicated through Intelligence and Information Sharing and Dissemination
Counter-Terror Investigation and Law Enforcement	Information needed by Counter-Terror Investigation and Law Enforcement to conduct investigations is provided through Intelligence and Information Sharing and Dissemination
Intelligence Analysis and Production	Intelligence and Information Sharing and Dissemination provides the means for communicating data that is gathered to those that analyze it in Intelligence Analysis and Production
Planning	Information provided via Intelligence and Information Sharing and Dissemination is used to ensure that plans adequately address terrorist threats
CBRNE Detection	Information from CBRNE Detection is transferred to the appropriate parties through Intelligence and Information Sharing and Dissemination
Community Preparedness and Participation	Community participation in awareness is one means by which information to be shared is generated.
Communications	Communications provides the necessary structure and systems for implementing Intelligence and Information Sharing and Dissemination.

Capability Activity Process Flow



`

Resource Element Description

Resource Elements	Components and Description
Personnel for sharing operational information	Personnel involved in the operational aspects of information sharing (e.g., information technology (IT) personnel, law enforcement, public health, fire, emergency medical service (EMS), transportation, and other non-law enforcement personnel)
Personnel for sharing information on collaborative initiatives	Federal, State, local, tribal, private sector personnel, and other key stakeholders involved in information sharing and collaboration initiatives
Joint Terrorism Task Forces (JTTFs)	Task forces 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)
Fusion center/process personnel	Supervisors and other management personnel within fusions centers involved in the oversight and execution of defined processes and procedures
Equipment and systems for information sharing and collaboration	Information sharing network architecture (e.g., Regional Information Sharing System (RISS)/Law Enforcement Online (LEO), Joint Regional Information Exchange System (JRIES), National Law Enforcement Telecommunication System (NLETS), FBI Criminal Justice Information System/National Crime Information Center (CJIS/NCIC) networks), including hardware and software physical and network security
Information sharing software	Data synthesis software (hazard prediction, assessment, and threat modeling software); data collection/information gathering 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. Initial planning, however, has been 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.

- 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
Personnel for sharing operational information	Personnel	As Needed		Federal/State Local	Incorporate All Stakeholders in Information Flow Vertically Flow Information Horizontally Flow Information
Personnel for sharing information on collaborative initiatives	Personnel	As Needed		Federal/State/ Local	All Activities
Joint Terrorism Task Forces (JTTFs)	Personnel	As Needed		Federal/State/ Local	All Activities
Fusion center/process personnel	Personnel	As Needed		Federal/State/ Local	All Activities
Equipment and systems for information sharing and collaboration	Equipment	As Needed		Federal/State/ Local	All Activities
Information Sharing 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.
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.
8. *Applying Security Practices to Justice Information Sharing.* 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.
9. *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.
10. *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.
11. *The 9/11 Commission Report.* National Commission on Terrorist Attacks upon the United States. July 2004. http://www.9-11commission.gov/.
12. The Homeland Security Advisory Council Prevention and Information Sharing Working Group. 2004.
13. Fusion Center Initiative. Homeland Security Advisory Council. April 2005.
14. State, Tribal and Local Intelligence and Information Sharing Initiative. Homeland Security Advisory Council. December 2004.
15. Homeland Security Advisory Council. June 2005.
16. *National Strategy for Homeland Security*. Office of Homeland Security. July 2002. http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.
17. Sector-Specific Intelligence Sharing Analysis Center information. Department of Homeland Security.
18. Homeland Security Information Network. http://www.dhs.gov/dhspublic/display?theme=43&content=3747&print=true.
19. Information Sharing and Analysis Center program. http://www.isaccouncil.org/about/.
20. *NFPA 1061: Standard for Professional Qualifications for Public Safety Telecommunicator*. National Fire Protection Association. 2002. http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1061
21. *NFPA 1221: Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*. National Fire Protection Association. 2002. http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1221
22. *NFPA 1561: Standard on Emergency Services Incident Management System. National Fire Protection Association. 2005. http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=15*