



JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

INTELLIGENCE GUIDE FOR FIRST RESPONDERS



JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

INTELLIGENCE GUIDE
FOR FIRST RESPONDERS

LEGAL DISCLAIMER

Nothing in this handbook shall be construed to impair or otherwise affect the authority granted by law to a department or agency, or the head thereof. Additionally, the handbook is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States; its departments, agencies, or entities; its officers, employees, or agents; or any other person.

“STATE, LOCAL, AND TRIBAL GOVERNMENTS ARE CRITICAL PARTNERS IN SECURING AND DEFENDING THE UNITED STATES FROM TERRORISM AND OTHER THREATS TO THE UNITED STATES AND ITS INTERESTS. OUR NATIONAL INTELLIGENCE EFFORT SHOULD TAKE INTO ACCOUNT THE RESPONSIBILITIES AND REQUIREMENTS OF STATE, LOCAL, AND TRIBAL GOVERNMENTS AND, AS APPROPRIATE, PRIVATE SECTOR ENTITIES, WHEN UNDERTAKING THE COLLECTION AND DISSEMINATION OF INFORMATION AND INTELLIGENCE TO PROTECT THE UNITED STATES.”

EXECUTIVE ORDER 12333

INTRODUCTION

In the post-9/11 era, first responders have incorporated protecting the Homeland against terrorism into their daily mission. Law enforcement, fire service, and emergency medical services personnel play a vital role in detecting and preventing attacks because of the nature of their work, their frequent interaction with members of the public, and the level of access their jobs provide. People who hold these jobs often can identify behaviors or activities that could signal a pending terrorist attack; therefore, public safety personnel must continue to report, according to the Nationwide Suspicious Activity Reporting Initiative, observations that raise reasonable suspicion.

The Intelligence Community routinely produces information for public safety personnel that may help first responders identify terrorist-related activities and prevent, deter, or respond to terrorist attacks. You can obtain this information through existing joint partnerships and from Internet-based U.S. Government information-sharing systems. It is critical that first responders, who are entrusted with keeping our citizens safe, be able to access, understand, and use this information.

The Joint Counterterrorism Assessment Team (JCAT)¹ **Intelligence Guide for First Responders** was produced by first responders for first responders and was designed to improve information sharing among state, local, tribal, and territorial jurisdictions and the federal government. This reference aid will accomplish the following:

- Highlight your role and responsibility as a consumer of intelligence information
- Demonstrate how to handle this information and why it must be protected
- Show you where to find this information and how to gain access to Internet-based U.S. Government systems
- Help you understand and participate in the Nationwide Suspicious Activity Reporting Initiative
- Provide an overview of the Intelligence Community, the intelligence cycle, and the products available to you
- Identify existing federal, state, local, tribal, and territorial partnerships that you can use to carry out your duties and responsibilities

¹ JCAT consists of state, local, tribal, and territorial first responders and public safety professionals from around the country, working side by side with federal intelligence analysts from the National Counterterrorism Center (NCTC), Department of Homeland Security (DHS), and Federal Bureau of Investigation (FBI) to research, produce, and disseminate counterterrorism intelligence. We offer federal fellowship opportunities to public safety professionals—law enforcement, emergency medical services, fire service, intelligence, homeland security, and public health officials—from state, local, tribal, and territorial government agencies. For more information, please visit us at www.nctc.gov/jcat.html.

During 2007-14, the following jurisdictions were represented in JCAT and in the Interagency Threat Assessment and Coordination Group (JCAT's predecessor):

ABINGTON POLICE DEPARTMENT, PA

LITTLE RIVER BAND OF OTTAWA INDIANS, MI

ALBUQUERQUE POLICE DEPARTMENT, NM

MARICOPA COUNTY DEPARTMENT OF HEALTH, AZ

ARLINGTON POLICE DEPARTMENT, TX

MINNEAPOLIS POLICE DEPARTMENT, MN

ATLANTA POLICE DEPARTMENT, GA

NATIONAL COUNTERTERRORISM CENTER

AURORA POLICE DEPARTMENT, CO

NEBRASKA HEALTH AND HUMAN SERVICES, NE

BOSTON POLICE DEPARTMENT, MA

NEW HANOVER COUNTY SHERIFF'S OFFICE, NC

CITY OF PHOENIX FIRE DEPARTMENT, AZ

NEW JERSEY STATE POLICE, NJ

FAIRFAX COUNTY FIRE AND RESCUE DEPARTMENT, VA

OAKLAND COUNTY SHERIFF'S OFFICE, MI

FEDERAL BUREAU OF INVESTIGATION

OHIO STRATEGIC ANALYSIS AND INFORMATION CENTER, OH

FIRE DEPARTMENT CITY OF NEW YORK, NY

ONEIDA INDIAN NATION POLICE, NY

FLORIDA DEPARTMENT OF HEALTH, FL

ORANGE COUNTY SHERIFF'S OFFICE, CA

FLORIDA HIGHWAY PATROL, FL

PHILADELPHIA POLICE DEPARTMENT, PA

HARRIS COUNTY SHERIFF'S OFFICE, TX

PHOENIX POLICE DEPARTMENT, AZ

HENNEPIN COUNTY SHERIFF'S OFFICE, MN

SEATTLE FIRE DEPARTMENT, WA

HOUSTON FIRE DEPARTMENT, TX

U.S. DEPARTMENT OF HOMELAND SECURITY

ILLINOIS STATE POLICE, IL

WASHINGTON STATE PATROL, WA

INDIANA STATE POLICE, IN

WASHINGTON D.C. FIRE AND EMS DEPARTMENT

LAS VEGAS METRO POLICE DEPARTMENT, NV

WASHINGTON D.C. METROPOLITAN POLICE DEPARTMENT

LOS ANGELES POLICE DEPARTMENT, CA



CONTENTS

HOW TO

| | |
|----|---|
| 1 | Handling Sensitive But Unclassified Information |
| 5 | Gaining Access to Intelligence Community Information |
| 11 | Understanding Estimative Language |
| 13 | Reporting Suspicious Activity with a Nexus to Terrorism |

GENERAL INFORMATION

| | |
|----|---|
| 19 | What Is Intelligence? |
| 23 | What Intelligence Can and Cannot Do |
| 25 | The Intelligence Community |
| 29 | The Intelligence Cycle |
| 33 | Categories of Finished Intelligence |
| 35 | Intelligence Products Typically Available to First Responders |
| 39 | Joint Partnerships |

REFERENCES

| | |
|----|----------------------------|
| 45 | Terminology |
| 53 | Acronyms and Abbreviations |

SECTION ONE
HOW TO



**HANDLING SENSITIVE BUT UNCLASSIFIED
INFORMATION**

“OUR NATION’S DEFENSE DEPENDS IN PART ON THE FIDELITY OF THOSE ENTRUSTED WITH OUR NATION’S SECRETS.”

PRESIDENT BARACK OBAMA, 2013

HANDLING SENSITIVE BUT UNCLASSIFIED INFORMATION

Federal agencies routinely generate, use, store, and share information that is sensitive enough to require some level of protection. First responders should be aware of the handling requirements for sensitive information to ensure that only those who need it can use it and only for its intended purpose.

Government agencies continue to use dissemination control markings such as FOR OFFICIAL USE ONLY, LAW ENFORCEMENT SENSITIVE, PERSONALLY IDENTIFIABLE INFORMATION AND SENSITIVE SECURITY INFORMATION.

FOR OFFICIAL USE ONLY (FOUO) is not a classification but one of the most widely used dissemination control markings. Agencies throughout the government typically, though not consistently, use this marking to identify unclassified but sensitive information that may or may not otherwise be categorized by statute or regulation. Unauthorized disclosure of this information could negatively affect a person’s privacy or welfare, the way federal programs are conducted, or other programs or operations essential to the national or other government interests.

Dissemination of FOUO information is typically restricted to persons with a “need to know,” which is defined as “the determination made by an authorized holder of information that a prospective recipient requires access in order to perform or assist in a lawful and authorized governmental function (that is, access is required for the performance of official duties).” Other FOUO requirements include the following:

- FOUO information will not be disseminated in any manner— orally, visually, or electronically—to unauthorized personnel.
- The holder of the information will comply with access and dissemination restrictions.
- The recipient of FOUO information will have a valid need to know, and precautions will be taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

FOUO is used in the Intelligence Community to mark unclassified official government information that is withheld from public release until approved for release by the originator. It can be used by all agencies, and each agency can provide further guidance on handling procedures.

INFORMATION LABELED FOUO OR WITH ANY OTHER CONTROL MARKING NEEDS TO BE SAFEGUARDED AND WITHHELD FROM PUBLIC RELEASE UNTIL THE ORIGINATING AGENCY CLARIFIES THE NATURE OF THE HANDLING REQUIREMENTS OR APPROVES IT FOR PUBLIC RELEASE.

LAW ENFORCEMENT SENSITIVE (LES) refers to unclassified information originated by agencies with law enforcement missions that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence, or the integrity of pretrial investigative reports. Any law enforcement agency employee or contractor performing assigned duties may label information as LES if he or she is authorized by department-specific policy and directives.

LES is a content indicator and handling caveat that indicates the information was compiled for law enforcement purposes and contains operational law enforcement information or information that would reveal sensitive investigative techniques. You can release or disclose LES information to foreign persons, organizations, or governments only if you have *previous approval* from the originating agency and follow all Office of the Director of National Intelligence foreign sharing agreements and directives.

Agencies that *originate* LES information may choose to disseminate the information they have caveated by posting it on a website on a classified network or on an unclassified virtual private network with proper access controls. However, if the originating agency chooses to disseminate the information only on a point-to-point basis, the warning statement must be expanded to include the statement:

“Recipients are prohibited from subsequently posting the information marked LES on a website or an unclassified network.”

You cannot use information carrying the LES warning statement in legal proceedings without first receiving authorization from the originator. The originating organization may authorize other sharing of LES information (for example, with victims of a crime) when the specific circumstances justify it. If such a request is granted, the individual sharing the information must educate the recipient on how the information must be used and protected. Unclassified LES information is withheld from public release until approved for release by the originator.

PERSONALLY IDENTIFIABLE INFORMATION (PII) as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available in any medium and from any source that, when combined with other available information, could be used to identify an individual.

SENSITIVE SECURITY INFORMATION (SSI) is a specific category of sensitive but unclassified information that is governed by federal law. SSI is information obtained or developed which, if released publicly, would be detrimental to transportation security. SSI is not classified national security information and is not subject to the handling requirements governing such information, but is subject to the handling procedures required by the SSI Federal Regulation (49 CFR Part 1520). Unauthorized disclosure of SSI may result in civil penalties and other enforcement or corrective actions.



**ACCESSING INTELLIGENCE
COMMUNITY INFORMATION**

ACCESS TO UNCLASSIFIED INFORMATION

First responders can gain access to unclassified information through several systems and websites that require only that users perform homeland security or law enforcement activities on behalf of a state, local, tribal, or territorial government.

Strengthening SBU Information Sharing: Simplified Sign-On (SSO): Across the public safety community, authorized personnel need to have access to the right information at the right time to perform their duties. First responders must draw on complete information to make informed decisions before responding to an emergency, threat, tip, or lead. Independent organizations and their networks and services have this mission-critical information, but the Information Sharing Environment (ISE) bridges the gaps to enable seamless discovery of and access to information and services, including readily accessible information about officer safety, criminal intelligence, disaster coverage, and cyber threats.

Single sign-on (SSO)—also known as simplified sign-on—provides one of the underlying capabilities that make discovery and access easier. With SSO, users from one organization can gain access to multiple information sets and services from other organizations without needing to log in to different networks or requiring manual intervention. Operationalizing SSO has been a practical success story in the Sensitive But Unclassified (SBU) information-sharing arena. The members of the SBU Working Group can easily discover and gain access to mission services provided by other members of the group.

The SBU Working Group currently includes four core members: the DHS Homeland Security Information Network (HSIN), the FBI Law Enforcement Enterprise Portal (LEEP), Intelink, and the Department of Justice grant-funded State and Local Regional Information Sharing Systems Program (RISSNet). These members have created a trust network through operational and technical agreements allowing users of one system to gain access to the resources of another

system more seamlessly, responsibly, and securely than with previous approaches.

In operation today, an authorized RISSNet user can log on to RISSNet and gain access to resources on RISSNet, LEEP, Intelink, and HSIN without having to use another set of credentials or access method. A LEEP user can log on to LEEP and use resources in RISS and Intelink and so on. The goal is to take advantage of the success of connecting independent organizations to collaborate and share information. This also includes organizations that may not be formal members of the SBU Working Group. Recently, collaboration between LEEP and the Chicago Police Department enabled police officers to gain access to FBI's information resources, as well as the resources of other members of the SBU Working Group—RISS, HSIN, and Intelink—by using their existing login credentials.

Efforts are under way to expand access to additional services by identifying and providing incentives for new members to be part of the trust framework exemplified by the SBU Working Group. This approach to sharing and exchanging information among independent organizations enables stronger intelligence that strengthens the mission of the first responder community. Likewise, the SBU Working Group promotes additional information-sharing efforts, such as Security Trimmed Federated Search that allows organizations to share and gain access to information and, at the same time, safeguard the information by only returning results that the user performing the search is authorized to see.

There is much more to be done, but SSO is real and working today. If you have access to one of these systems (HSIN, RISS, LEEP, Intelink), we encourage you to explore the capabilities mentioned above. For additional information, please visit www.ise.gov.

Homeland Security Information Network (HSIN): The DHS Office of Intelligence and Analysis (I&A) continues to strengthen support for the National Network of Fusion Centers and for broader homeland security and law enforcement partners. To offer partners at all levels of government a forum for information sharing and analytic collaboration, I&A partnered with the Office of the Chief Information Officer to support the Homeland Security State and Local Intelligence Community of Interest transition to a new technology platform—Homeland Security Information Network (HSIN) Release 3 in 2013. HSIN is a national, secure, and trusted web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private-sector, and international partners engaged in the homeland security mission. 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 and is made up of a growing network of sites called Communities of Interest (COI). COIs are organized by state organizations, federal organizations, or mission areas, such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed using <https://hsin.dhs.gov/>.

HSIN-Intelligence (HSIN-Intel): HSIN-Intel is a COI within HSIN. The purpose of HSIN-Intel is to provide stakeholders across the Homeland Security Enterprise a platform for effective and efficient collaboration for tiered secure access to data, analytic exchange, and timely information sharing and situational awareness.

- HSIN-Intel, as the designated unclassified intelligence-sharing portal for DHS and its homeland security partners, serves as the principal platform for consolidation and interoperability with DHS information-sharing portals. HSIN-Intel is the only federal portal that provides intelligence information sharing between DHS and its federal, state, local, tribal, and territorial partners across the full spectrum of homeland security missions.
- HSIN-Intel COI membership is open to all those who collaborate on homeland security-related analytic issues, analysts, and personnel from federal, state, local, tribal, and territorial law enforcement and homeland security communities, as well as the National Network of Fusion Centers.

To request HSIN-Intel access, send an e-mail to the HSIN-Intel team at HSIN.Intel@hq.dhs.gov with the following information:

- >> Name
- >> Affiliated organization
- >> Official/business e-mail address
- >> Official/business phone number
- >> Brief justification

Minimum eligibility requirements include the following:

- >> Be a U.S. citizen
- >> Be a full-time, current employee (government or contractor personnel) of a law enforcement, criminal justice, emergency responder, or homeland security federal, state, local, tribal, or territorial government agency engaged in seeking to detect, defeat, or deter terrorist acts
- >> Have a government e-mail address (or other e-mail address approved by the state, territory, or urban area point of contact and the HSIN Intel Chief or designee)

If you would like access to other COIs, follow these instructions:

- >> From the main HSIN screen, hover over the “About” menu
- >> Click on “Communities.” Read through the text and click on “Site Directory” to see other COIs to which you may want to gain access

SitAware—The National Situation Awareness Room:

HSIN-Intel contains within its utilities suite an online conferencing, meeting, and intelligence-sharing application called Connect, which is a program created by Adobe to host online meetings, briefings, and training sessions in real time. Dedicated to providing updated intelligence and related information briefings during periods of regional crisis or during a national emergency, the HSIN Situation Awareness Room (SitAware) provides a meeting and information portal for analytic staff and law enforcement personnel to monitor and post relevant items during an incident of national or regional significance. SitAware is already established as a room within the HSIN-Connect portal to assist in responding to large-scale incidents, significantly elevated terrorist threats, or large national events, such as a general election, large sporting event, or inauguration. You can use your HSIN user name and password to log in to the site at <https://share.dhs.gov/sitaware>.

If you want to use the National Situation Awareness Room on your mobile device, follow these instructions:

- » Download the Adobe Connect mobile application to your smartphone
- » Type the following into the application address:
share.dhs.gov/sitaware
- » Use your HSIN user name and password to log in

Intelink-U: Intelink-U is the Intelligence Community's SBU information-sharing network. Content is provided by the Intelligence Community, other government agencies, foreign partners, academics, and open sources. Individuals with federal, state, local, tribal, and territorial homeland security and law enforcement responsibilities can request accounts at <https://www.intelink.gov>.

Law Enforcement Enterprise Portal (LEEP): You can use LEEP on any computer with an internet connection. This official government information-sharing and electronic-communications portal currently provides SSO access to LEO, RISSNet, the Joint Automated Booking System (JABS), the National Gang Intelligence Center (NGIC), eGuardian, the Internet Crime Complaint Center (IC3), the National Data Exchange (N-DEX), Intelink, and the U.S. Department of Justice myFX. You can find LEEP at <https://www.cjis.gov>.

Law Enforcement Online (LEO): Law Enforcement Online (LEO) is a secure, Internet-based information-sharing system for agencies around the world involved in law enforcement, first response, criminal justice, counterterrorism, and intelligence. With LEO, members can access or share SBU information anytime and anywhere, from any computer system with an Internet connection. This official government information-sharing and electronic-communications platform provides FBI, joint FBI and DHS, NCTC, and non-federally produced intelligence products at the LES/FOUO level. LEO also provides members access to tactical tools, such as the Virtual Command Center, ORION, Trax, and the National Alert System. Federal, state, local, tribal, and territorial personnel performing homeland security or law enforcement duties and foreign law enforcement personnel can request accounts.

Here are just a few examples of what is available to all levels of law enforcement, criminal justice, and public safety communities on LEO:

- » **Virtual Command Center (VCC):** A real-time situational awareness tool that can help law enforcement and other authorities during many situations, such as special public events, warrant sweeps, investigations, and natural disasters.
- » **Law Enforcement Online Special Interest Groups (LEOSIGs):** Allow members to participate in COIs to securely share information and receive specialized training.
- » **Virtual Office:** Enables agencies to store and retrieve information needed on scene and gain access to that information from any Internet connection, eliminating the need for an officer to travel to a physical office.
- » **Active Shooter Initiative:** The FBI Active Shooter Resources page provides a clearinghouse for materials available to law enforcement agencies and other first responders around the country to ensure preparedness for active-shooter cases and mass-casualty incidents.

Thanks to LEEP, access to LEO has been streamlined, and you can find critical law enforcement information in one location. In addition to the individual accounts that LEO grants, LEEP can provide access to entire law enforcement agencies, which means every member of an agency can have access to LEEP's many services.

OpenSource.gov: The Open Source Center (OSC) and its partners provide timely and tailored translations, reporting, and analysis on foreign policy and national security issues. The website features reports and translations from thousands of publications, television and radio stations, and Internet sources around the world. Also among the site's holdings are a foreign video archive and fee-based commercial databases for which OSC has negotiated licenses. OSC's reach extends from hard-to-find local publications and video to reports from some of the most renowned thinkers on national security issues inside and outside the U.S. Government. Federal, state, and local government employees and contractors can apply for an account at <http://www.opensource.gov>.

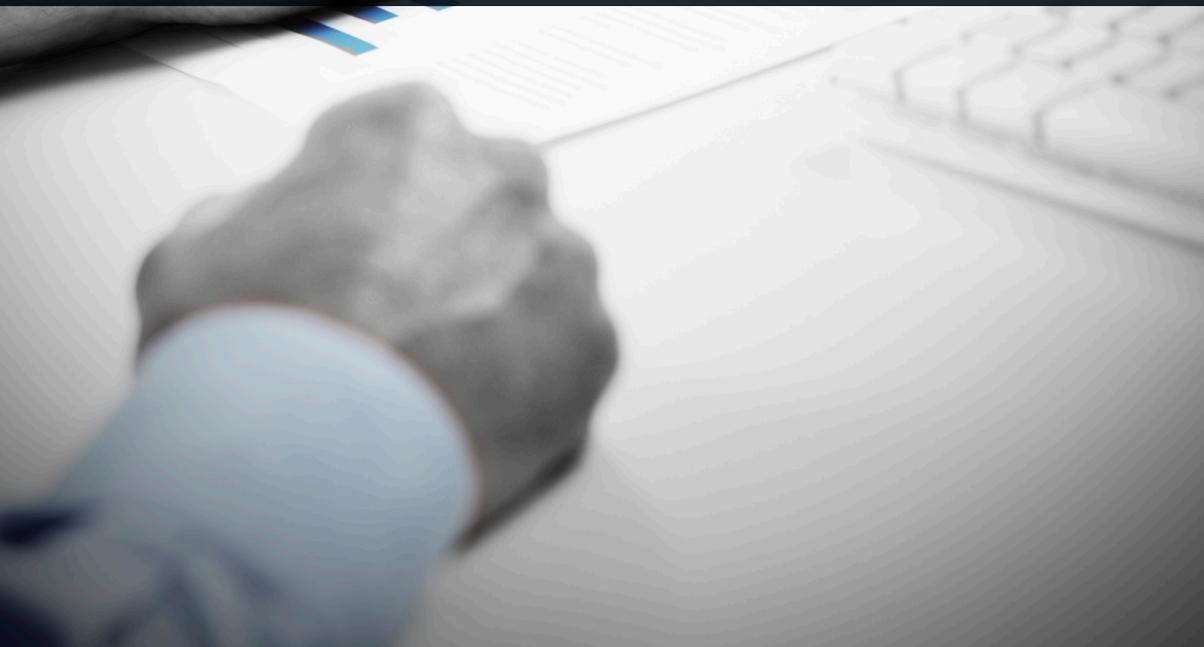
Regional Information Sharing Systems Network (RISSNET): RISSNet facilitates information sharing within the law enforcement community to combat criminal activities and conspiracies that take place in several jurisdictions. It contains six multistate intelligence centers (RISS Intelligence Centers), and members include federal, state, local, tribal, and territorial law enforcement agencies. You can request access through the regional RISS Intelligence Centers or apply online at <http://www.riss.net>.

Technical Resources for Incident Prevention (TRIPwire):

TRIPwire is DHS'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. TRIPwire combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to help law enforcement officials anticipate, identify, and prevent IED incidents. You can find more information at <https://www.tripwire.dhs.gov/IED>, or by contacting the Office for Bombing Prevention at OBP@dhs.gov or through the TRIPwire help desk at help@tripwire-dhs.net.



UNDERSTANDING ESTIMATIVE LANGUAGE



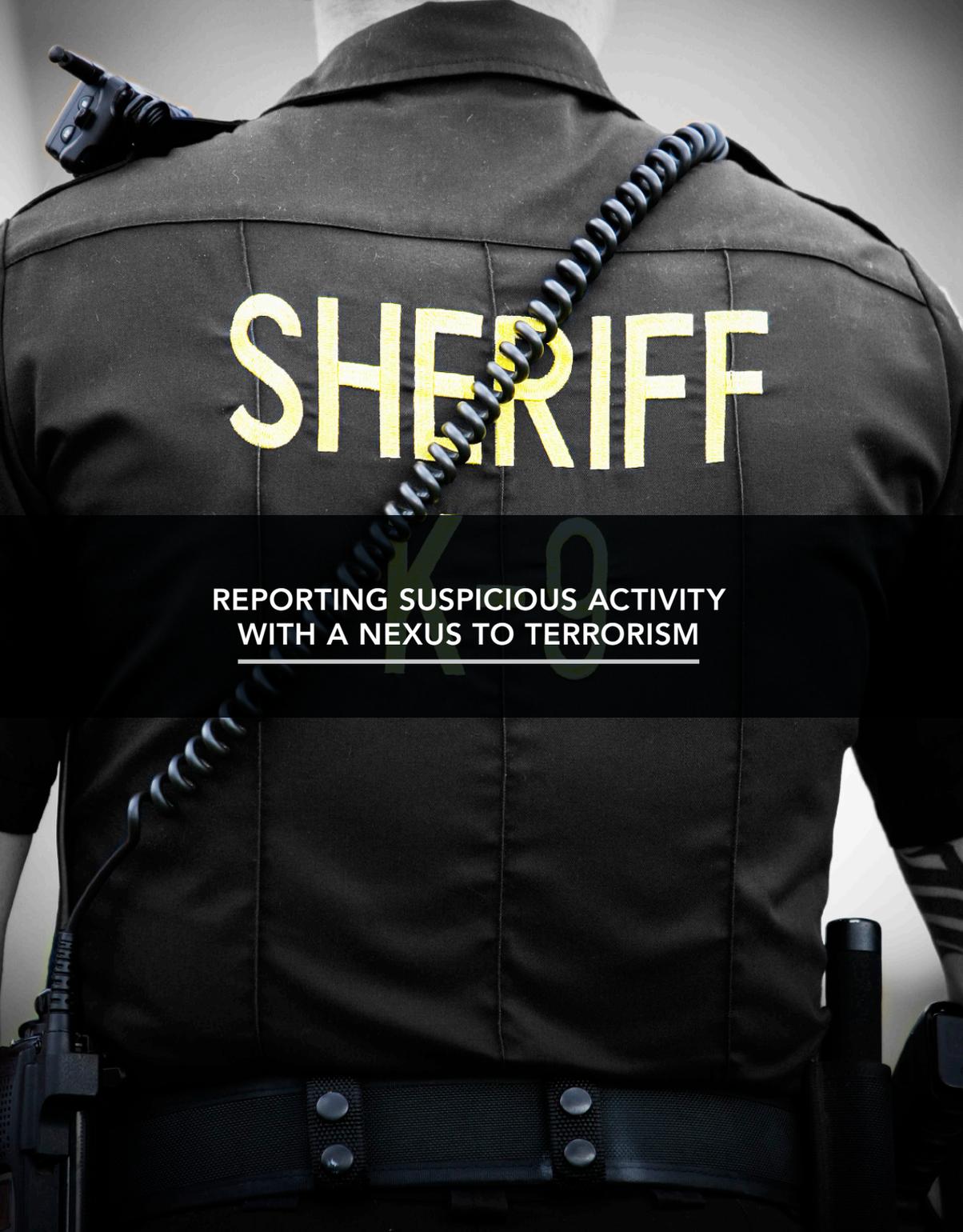
THE USE OF JUDGMENTS

When the Intelligence Community (IC) uses phrases such as “we judge” or “we assess”—used synonymously—as well as “we estimate,” “likely,” or “indicate,” the IC is trying to convey an analytic assessment or judgment. These assessments, which analysts must base on incomplete or at times fragmentary information, are not facts, proof, or knowledge. Analysts base some judgments directly on collected information; others rest on assessments that serve as building blocks. In either type of judgment, the IC does not have “proof” that shows something to be a factor that definitively links two items or issues.

Intelligence judgments pertaining to likelihood reflect the community’s sense of the probability of a development or event. The IC does not intend the term “unlikely” to imply that an event will not happen. It uses “probably” and “likely” to indicate that there is a greater than even chance. The IC uses phrases such as “we cannot dismiss,” “we cannot rule out,” and “we cannot discount” to reflect an unlikely—or even remote—event whose consequences are such that it warrants mentioning. Words such as “may be” and “suggest” are used to reflect situations in which the IC cannot assess the likelihood generally because relevant information is nonexistent, sketchy, or fragmented.

In addition to using words within a judgment to convey degrees of likelihood, the IC also ascribes “high,” “moderate,” or “low” confidence levels according to the scope and quality of information supporting analytic judgments.

- **HIGH CONFIDENCE** generally indicates that the IC’s judgments are based on high-quality information or that the nature of the issue makes it possible to develop a solid judgment.
- **MODERATE CONFIDENCE** generally means that the information could be interpreted in various ways, that the IC has alternative views, or that the information is credible and plausible but not corroborated sufficiently to justify a higher level of confidence.
- **LOW CONFIDENCE** generally means that the information is scant, questionable, or very fragmented, so it is difficult to make solid analytic inferences; it could also mean that the IC has significant concerns about or problems with the sources.

The image shows the back of a person wearing a dark, short-sleeved uniform shirt. The word "SHERIFF" is printed in large, bold, yellow capital letters across the upper back. A black coiled radio cord is draped over the shoulder and across the back. A black radio is clipped to the left shoulder. At the bottom, a black tactical belt is visible with several pouches and a handgun holstered on the right side. The background is a plain, light-colored wall.

SHERIFF

**REPORTING SUSPICIOUS ACTIVITY
WITH A NEXUS TO TERRORISM**

“WE WILL CONTINUE TO INTEGRATE AND LEVERAGE STATE AND MAJOR URBAN AREA FUSION CENTERS THAT HAVE THE CAPABILITY TO SHARE CLASSIFIED INFORMATION AND IMPLEMENT AN INTEGRATED APPROACH TO OUR COUNTERTERRORISM INFORMATION SYSTEM TO ENSURE THAT THE ANALYSTS, AGENTS, AND OFFICERS WHO PROTECT US HAVE ACCESS TO ALL RELEVANT INTELLIGENCE THROUGHOUT THE GOVERNMENT. WE ARE IMPROVING INFORMATION SHARING AND COOPERATION BY LINKING NETWORKS TO FACILITATE FEDERAL, STATE, AND LOCAL CAPABILITIES TO SEAMLESSLY EXCHANGE MESSAGES AND INFORMATION, CONDUCT SEARCHES, AND COLLABORATE.”

NATIONAL SECURITY STRATEGY, DECEMBER 2012

REPORTING SUSPICIOUS ACTIVITY WITH A NEXUS TO TERRORISM

Because of the nature of their work, the more than 800,000 law enforcement officers and 1.2 million firefighters in the U.S. are positioned to identify activities that may be associated with terrorism. In many instances, information based on suspicious behavior has led to the disruption of a terrorist attack, the arrest of individuals intending to do harm, or the corroboration of existing intelligence. It is of utmost importance that information on suspicious activities be shared with and between federal, state, local, tribal, territorial, and private-sector partners.

SUSPICIOUS ACTIVITY REPORTS (SARS) SHOULD BE MADE AVAILABLE TO THE JOINT TERRORISM TASK FORCES (JTTFs) AND TO YOUR LOCAL AREA FUSION CENTERS IN A TIMELY MANNER.

The Nationwide Suspicious Activity Reporting Initiative

(NSI): The NSI is a collaborative effort led by the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) in partnership with state, local, tribal, and territorial law enforcement and hometown partners. The NSI provides law enforcement and homeland security agencies with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing terrorism-related information.

THE PROTECTION OF PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES (P/CRCL) IS PARAMOUNT TO THE SUCCESS OF THE NSI. GIVEN THIS IMPORTANCE, THE NSI HAS WORKED WITH VARIOUS ADVOCACY GROUPS AND OTHER STAKEHOLDERS TO DEVELOP PROTECTIONS THAT, WHEN CONSOLIDATED, MAKE UP A COMPREHENSIVE NSI PRIVACY PROTECTION FRAMEWORK.

THESE EFFORTS HAVE SERVED AN IMPORTANT ROLE IN SUCCESSFULLY SHAPING NSI POLICIES AND PROCESSES.

What Is an Information Sharing Environment SAR

(ISE-SAR) and Why Is It Important? The Information Sharing Environment (ISE)—SAR Functional Standard v.1.5.5 defines *suspicious activity* as “observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.” This definition was developed after critical input from several privacy, civil rights, and civil liberties

advocacy groups. The SAR process is critical to sharing information about suspicious activity with a potential nexus to terrorism, which can help prevent terrorist attacks and other related criminal activity from occurring.

Online ISE-SAR Training for Law Enforcement and

Hometown Security Partners: The NSI training strategy is a multifaceted approach designed to increase the effectiveness of state, local, and tribal law enforcement and public safety professionals and other frontline partners in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. The SAR Line Officer Training and each sector-specific SAR Hometown Security Partners Training discuss how to report identified suspicious activity to the proper authorities while maintaining the protection of citizens’ privacy, civil rights, and civil liberties. Online training is available on the NSI website (http://nsi.ncirc.gov/training_online.aspx) and includes:

- Scenarios to help illustrate the benefit and importance of suspicious activity reporting
- Descriptions of SAR-related behaviors and indicators

Ten Ways To Integrate SARs Into Your Agency’s Operations

- **RECOGNIZE** the importance of SARs, understand your role in the SAR process, and know that your involvement makes a difference. Strong leadership is an essential element.

Gain support from personnel, leaders, and policymakers both internally and externally.

- **DEVELOP** a data collection process and a secure standardized reporting format for sharing suspicious activity. Review other agencies' SAR process missions/ standard operating procedures to better understand the process and identify promising practices. Define and communicate trends in terrorism-related activity, geographically specific threat reporting, dangers to critical infrastructure, and general situational awareness.
- **ADOPT** common national standards to enhance your capability to quickly and accurately analyze suspicious activity data, such as the ISE-SAR Functional Standard, the National Information Exchange Model, and the records management system and computer-aided dispatch functional standards.
- **INCORPORATE** appropriate guidelines and concepts into your operations, such as the National Criminal Intelligence Sharing Plan, the Fusion Center Guidelines, the Findings and Recommendations of the SAR Support and Implementation Project, and privacy and civil liberties templates. Use these guidelines to establish and integrate the SAR process.
- **IMPLEMENT** and adhere to your agency's privacy policy, and ensure that the privacy, civil rights, and civil liberties of citizens are protected. Evaluate your privacy policy and update it, if necessary, to ensure that it specifically addresses gathering, documenting, processing, and sharing information regarding terrorism-related criminal activity. Ensure that the privacy policy is transparent, and communicate the policy to the public and stakeholders.
- **TRAIN** all agency personnel on the SAR process, and institutionalize it within your agency. Ensure that law enforcement and public safety personnel understand the SAR process and what internal policies or protocols exist to share appropriate information. Familiarize yourself with available training classes to enhance capabilities, such as the NSI training programs available at <http://nsi.ncirc.gov> or the State and Local Anti-Terrorism Training (SLATT®) Program available at www.SLATT.org.
- **INSTITUTIONALIZE** the gathering of suspicious activity information at the street level, and standardize the reporting of such data so that it may be shared with the JTF and other appropriate public safety partners, such as your criminal intelligence unit or the state or regional fusion center. Once your agency's SAR process has been developed,

continual improvements will ensure the integrity and institutionalization of the process within your agency.

- **EDUCATE** citizens, businesses, and partners on suspicious activity reporting and how to report activity to the appropriate officials. Consider instituting a Building Communities of Trust (BCOT) program to engage community leaders in your efforts. Guidance on how to establish a BCOT program is available at http://nsi.ncirc.gov/documents/BCOT_Fact_Sheet.pdf. Develop outreach materials to educate the public on recognizing and reporting behaviors and incidents that point toward terrorism or other criminal activity. Existing SAR awareness training programs, such as NSI's Hometown Security Partners training programs available at http://nsi.ncirc.gov/training_online.aspx, can be used to educate those partners with missions similar to law enforcement.
- **PARTNER** with other law enforcement, public safety, private-sector, and state or major urban area fusion centers. Foster interagency collaboration to maximize resources and create an effective and efficient information-sharing environment.
- **CONNECT** to a major information-sharing network, such as RISSNet, LEO, or HSIN. Take advantage of proven and trusted technology to share information, communicate, and gain access to additional resources.

For additional information go to: <http://nsi.ncirc.gov>.

The nationwide "**If You See Something, Say Something™**" public awareness campaign is a simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime and to emphasize the importance of reporting suspicious activity to the proper local law enforcement authorities. DHS launched the campaign in conjunction with NSI to train members of state and local law enforcement to recognize behaviors and indicators related to terrorism and terrorism-related crime, standardize how those observations are documented and analyzed, and ensure the sharing of those reports with the FBI-led JTFs for further investigation and fusion centers for analysis. A critical element of the DHS mission is to ensure that the privacy, 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 privacy, civil rights, and civil liberties by emphasizing behavior, rather than appearance, in identifying and reporting suspicious activity.

For more information, please go to: <http://www.dhs.gov/if-you-see-something-say-something> is interactive.

SECTION TWO

GENERAL INFORMATION



WHAT IS INTELLIGENCE?

“INTELLIGENCE INCLUDES THE ORGANIZATIONS, CAPABILITIES, AND PROCESSES INVOLVED IN COLLECTION, PROCESSING, EXPLOITATION, ANALYSIS, AND DISSEMINATION OF INFORMATION OR FINISHED INTELLIGENCE. INTELLIGENCE PRODUCTS PROVIDE USERS WITH THE INFORMATION THAT HAS BEEN COLLECTED AND ANALYZED BASED ON THEIR REQUIREMENTS.”

23 OCTOBER 2013 EDITION OF JOINT PUB 2-0, JOINT INTELLIGENCE

THE INTELLIGENCE COMMUNITY USES FIVE BASIC INTELLIGENCE DISCIPLINES

Geospatial intelligence (GEOINT) refers to the exploitation and analysis of imagery, imagery intelligence (IMINT), and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth.

Human intelligence (HUMINT) is intelligence derived from information collected and provided by human sources. This information includes overt data collected by personnel in diplomatic and consular posts as well as otherwise unobtainable information collected via clandestine sources, debriefings of foreign nationals and U.S. citizens who travel abroad, official contacts with foreign governments, and direct observation.

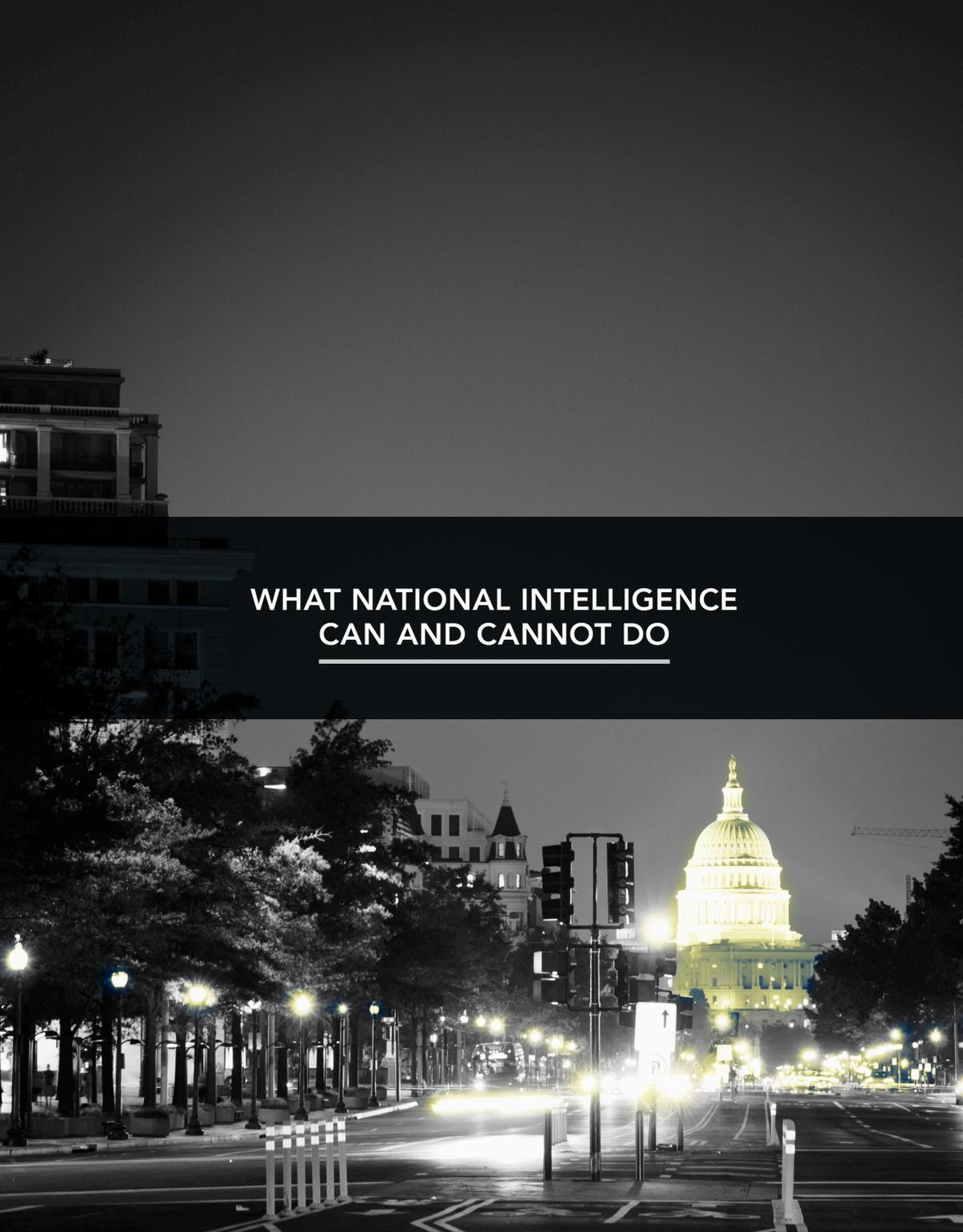
Measurement and signature intelligence (MASINT) is technically derived data other than imagery and signals intelligence (SIGINT). The data is analyzed and results in intelligence that locates, identifies, or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. Examples include the distinctive radar signatures of specific aircraft systems or the chemical compositions of air and water samples.

Open-source intelligence (OSINT) is produced from publicly available information collected, exploited, and disseminated in a timely manner to an appropriate audience to address a specific intelligence requirement. OSINT draws from a wide variety of information and sources, including the following:

- **Mass media**—newspapers, magazines, radio, television, and computer-based information.
- **Public data**—government reports, official data such as budgets and demographics, hearings, legislative debates, press conferences, speeches, directories, organization charts, marine and aeronautical safety warnings, environmental impact statements, contract awards, and required financial disclosures.
- **Gray literature** (a.k.a. grey literature)—open-source material that usually is available through specialized access for a specific audience; can include, but is not limited to, research reports, technical reports, economic reports, trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, studies, dissertations and theses, trade literature, market surveys, and newsletters; cuts across scientific, political, socioeconomic, and military disciplines.
- **Observation and reporting**—significant information not otherwise available that is or has been provided by amateur airplane spotters, radio monitors, and satellite observers, among many others; availability of worldwide satellite photography, often high resolution, on the Internet has expanded open-source capabilities into areas formerly available to major intelligence services only.

Signals intelligence (SIGINT) is gathered from data transmissions, including communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). SIGINT includes both the raw data and the analysis of the data.

- **COMINT** is the capture of information for the purposes of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, or analyzing the meaning of communications.
- **FISINT** is information derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems including, but not limited to, telemetry, beaconry, electronic interrogators, and video data links.
- **ELINT** is information derived primarily from electronic signals that do not contain speech or text (which are considered COMINT). The most common sources of this type of information are radar signals.



**WHAT NATIONAL INTELLIGENCE
CAN AND CANNOT DO**

“INFORMATION ON ITS OWN MAY BE OF UTILITY TO THE COMMANDER, BUT WHEN RELATED TO OTHER INFORMATION ABOUT THE OPERATIONAL ENVIRONMENT AND CONSIDERED IN THE LIGHT OF PAST EXPERIENCE, IT GIVES RISE TO A NEW UNDERSTANDING OF THE INFORMATION, WHICH MAY BE TERMED ‘INTELLIGENCE.’”

23 OCTOBER 2013 EDITION OF JOINT PUB 2-0, JOINT INTELLIGENCE

INTELLIGENCE INFORMATION CAN BE AN EXTREMELY POWERFUL TOOL

First responders will find national intelligence information most useful when they have a clear understanding of what it can and cannot do. While laws, policies, capabilities, and standards are constantly changing, these general guidelines can help first responders make the most of this resource.

WHAT NATIONAL INTELLIGENCE CAN DO

National intelligence can provide the following:

- Decision advantage, by presenting information and analysis that can improve the decisionmaking process for consumers of intelligence and partners while hindering that of our enemies
- Warning of potential threats
- Insight into key current events
- Situational awareness
- Long-term strategic assessments on issues of ongoing interest
- Pretravel security overviews and support
- Reports on specific topics, either as part of ongoing reporting or upon request for short-term needs
- Knowledge about persons of interest

WHAT NATIONAL INTELLIGENCE CANNOT DO

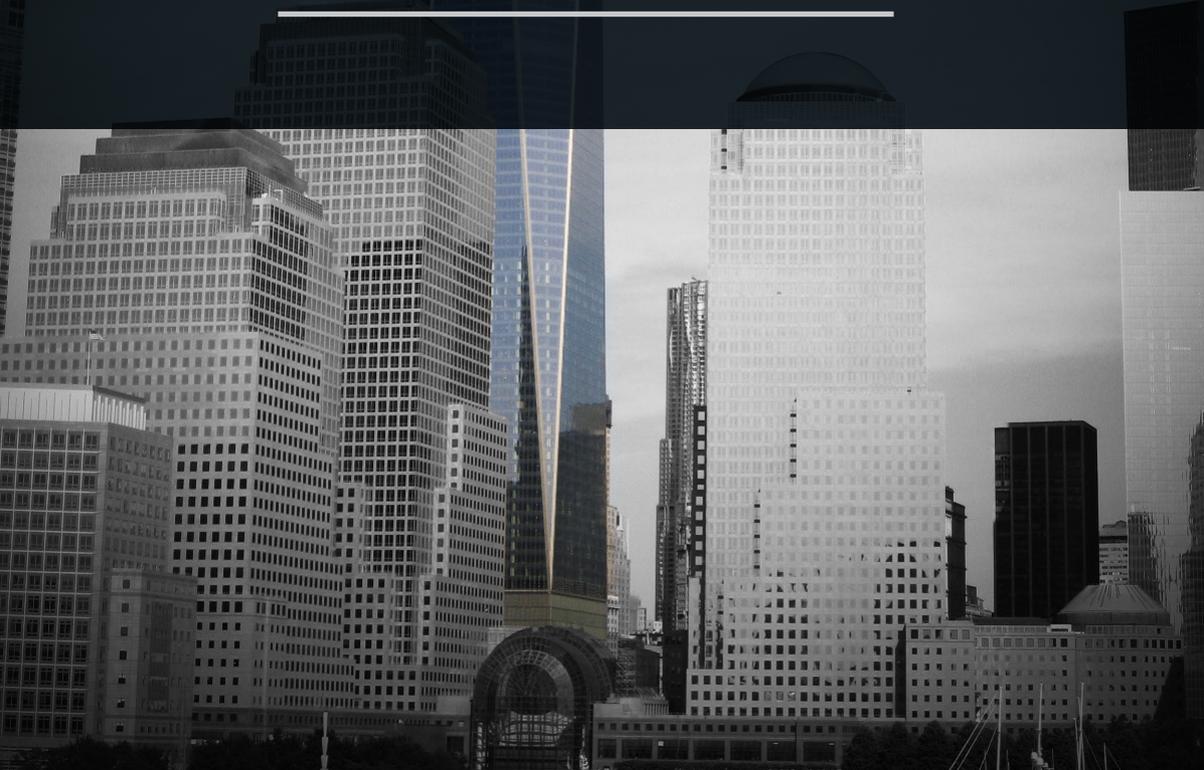
Realistic expectations will help consumers of intelligence fill their intelligence needs, but national intelligence cannot do the following:

- **Predict the future.** Intelligence can provide assessments of probable scenarios or developments, but there is no way to predict what will happen with absolute certainty.
- **Violate U.S. law.** IC activities must be consistent with all applicable laws and executive orders, including, the United States Constitution, the National Security Act of 1947, as amended; the Foreign Intelligence Surveillance Act; the Intelligence Reform and Terrorism Prevention Act; the Privacy Act of 1974; the Detainee Treatment Act; the Homeland Security Act of 2002, as amended; Executive Order 12333; and the Military Commission Act.

ALL ACTIVITIES OF THE IC ARE SUBJECT TO EXTENSIVE AND RIGOROUS OVERSIGHT BOTH WITHIN THE EXECUTIVE BRANCH AND BY THE LEGISLATIVE BRANCH, AS REQUIRED BY THE NATIONAL SECURITY ACT OF 1947, AS AMENDED.



THE INTELLIGENCE COMMUNITY



“THE INTELLIGENCE COMMUNITY EXISTS TO PROVIDE POLITICAL AND MILITARY LEADERS WITH THE GREATEST POSSIBLE DECISION ADVANTAGE. WE UNDERSTAND, NOW MORE THAN EVER, THAT THE BEST WAY TO ACCOMPLISH OUR GOAL IS THOROUGH INTEGRATION OF ALL NATIONAL INTELLIGENCE CAPABILITIES.”

JAMES R. CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE

THE U.S. INTELLIGENCE COMMUNITY

The Intelligence Community (IC) is a coalition of 17 agencies and organizations within the Executive Branch (as defined by the National Security Act of 1947, as amended) that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and protect national security. It includes other elements of the government that may be designated by the President or jointly by the Director of National Intelligence and the head of the department or agency concerned. The IC's primary mission is to collect and convey essential information the President and members of the policymaking, law enforcement, and military communities require to execute their appointed duties. Agencies such as the Central Intelligence Agency, Defense Intelligence Agency, and National Security Agency perform intelligence as their primary function, while other such as the Departments of State and Defense perform intelligence duties in addition to other primary functions. Some agencies focus on specific problem sets, use selected intelligence disciplines, or support a primary customer set, but their overall mission remains the same—to protect the U.S. and its interests.

THE ACTIVITIES OF THE IC INCLUDE THE FOLLOWING:

- Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities
- Production and dissemination of intelligence
- Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the U.S., international terrorist and international narcotics activities, and other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents
- Special activities
- Administrative and support activities within the U.S. and abroad necessary for the performance of authorized activities
- Such other intelligence activities as the President may direct from time to time

The IC comprises the following 17 agencies and organizations:





CENTRAL INTELLIGENCE AGENCY



DEFENSE INTELLIGENCE AGENCY



DEPARTMENT OF ENERGY, OFFICE OF INTELLIGENCE



DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INTELLIGENCE AND ANALYSIS



DEPARTMENT OF STATE, BUREAU OF INTELLIGENCE AND RESEARCH



DEPARTMENT OF THE TREASURY, TREASURY OFFICE OF TERRORISM AND FINANCIAL INTELLIGENCE



DRUG ENFORCEMENT ADMINISTRATION, OFFICE OF NATIONAL SECURITY INTELLIGENCE



FEDERAL BUREAU OF INVESTIGATION



NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY



NATIONAL RECONNAISSANCE OFFICE



NATIONAL SECURITY AGENCY



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE



U.S. AIR FORCE, AIR FORCE INTELLIGENCE



U.S. ARMY, ARMY INTELLIGENCE



U.S. COAST GUARD, COAST GUARD INTELLIGENCE



U.S. MARINE CORPS, MARINE CORPS INTELLIGENCE



U.S. NAVY, OFFICE OF NAVAL INTELLIGENCE



THE INTELLIGENCE CYCLE



THE INTELLIGENCE CYCLE

The term *intelligence cycle* refers to the five-step process of developing raw information into finished intelligence for policymakers, military commanders, and other consumers to use in making decisions. The cycle is highly dynamic and never ends, and it often includes a sixth stage of *evaluation*, sometimes referred to as *feedback*. Evaluation occurs for each of the stages individually and for the cycle as a whole.

STAGES OF THE INTELLIGENCE CYCLE:

- **PLANNING AND DIRECTION (or establishing the intelligence requirements for the consumer of intelligence):** The opening stage for the intelligence cycle, planning and direction serves as the springboard from which all intelligence activities are launched. The direction portion will most often come first, whereby the consumer of intelligence issues a requirement for a specific product—a report, graphic, or, at times, raw intelligence. From that, the intelligence organization being tasked will plan its activity.
- **COLLECTION (or gathering the raw data required to produce the finished product):** Collection is accomplished by using any combination of the five basic intelligence sources or disciplines (GEOINT, HUMINT, MASINT, OSINT, and SIGINT). The raw information gathered includes, but is not limited to, newspaper reporting, aerial imagery, satellite imagery, documents, electronic parameters, and more.
- **PROCESSING AND EXPLOITATION (or converting the raw data into a comprehensible form for use in the finished product):** Processing and exploitation involve the use of highly trained, specialized personnel and equipment to turn the data into usable and understandable information. Translation, decryption, and interpretation of film and imagery are only a few examples of the methods used to process film, magnetic, and other media that collect and store data.
- **ANALYSIS AND PRODUCTION (or integrating, evaluating, analyzing, and preparing processed information for the finished product):** Analysis and production require highly trained, specialized personnel—analysts—to give meaning and priority to the information. Synthesizing the processed information into actionable finished intelligence makes the information useful to the customer. It is important to note, however, that in some cases, the cycle may skip this stage; for example, when the consumer of intelligence needs only the factual reporting or raw imagery. During the Cuban Missile Crisis (October 1962), President Kennedy needed only the actual count of Soviet equipment in Cuba or facts concerning Soviet activity with no analysis, since that was implied by the numbers and activity reported.
- **DISSEMINATION (or delivering the finished product to the consumer who requested it and to others as applicable):** Dissemination is self-explanatory. Consumers of intelligence receive the finished product, usually via electronic transmission through websites, e-mail, or Web 2.0 collaboration tools, though sometimes in hardcopy. We refer to the final product as finished intelligence, and after it is disseminated, new intelligence gaps may be identified to prompt the intelligence cycle to begin again.
- **EVALUATION (or acquiring continual feedback to refine each stage and the cycle as a whole):** Constant evaluation and feedback from consumers enable those involved in the intelligence cycle to adjust and refine their activities and analysis to better meet consumers of intelligence's changing and evolving information needs.



CATEGORIES OF FINISHED INTELLIGENCE

“**A** MORE UNIFIED AND EFFECTIVE INTELLIGENCE COMMUNITY WILL ENHANCE THE NATION'S ABILITY TO SHARE INFORMATION WITH OUR LAW ENFORCEMENT AND PRIVATE SECTOR PARTNERS, AND WILL PREVENT AND MINIMIZE THREATS TO OUR NATIONAL SECURITY.”

JAMES COMEY, FBI DIRECTOR

THE FIVE CATEGORIES OF FINISHED INTELLIGENCE

Intelligence information that has been reviewed and correlated with data from other available sources is referred to as “finished intelligence” and disseminated directly to the customers whose initial needs generated the intelligence requirements and to others with a need to know. The consumers use the intelligence to make decisions that may lead to requests for further examination, thus triggering the intelligence cycle to begin again.

THE FIVE CATEGORIES OF FINISHED INTELLIGENCE CAN BE DESCRIBED AS FOLLOWS:

- **Current Intelligence** addresses day-to-day events. It details new developments and related background to assess their significance, warn of their near-term consequences, and signal potentially dangerous situations in the near future.
- **Estimative intelligence** looks forward to assess potential developments that could affect U.S. national security. By discussing the implications of a range of possible outcomes and alternative scenarios, estimative intelligence helps policymakers think strategically about long-term threats.
- **Warning intelligence** sounds an alarm or gives notice to customers. It suggests urgency and implies the potential need to respond with policy action. Warning intelligence includes identifying or forecasting events that could prompt the engagement of U.S. military forces or events that would have a sudden and detrimental effect on the Homeland or on U.S. foreign policy concerns. Warning analysis involves exploring alternative futures and low probability/high impact scenarios.
- **Research intelligence** includes studies that support both current and estimative intelligence.
- **Scientific and technical intelligence** includes an examination of the technical development, characteristics, performance, and capabilities of foreign technologies, including weapon systems or subsystems. This category covers a complete spectrum of sciences, technologies, weapon systems, and integrated operations.

A black and white photograph of three firefighters in full protective gear, including helmets and oxygen tanks, standing in front of a large, intense fire. The firefighters are seen from the back and side, looking towards the flames. The fire is bright yellow and orange, contrasting sharply with the dark background. The scene is dramatic and emphasizes the bravery of first responders.

**INTELLIGENCE PRODUCTS TYPICALLY
AVAILABLE TO FIRST RESPONDERS**

INTELLIGENCE FOR FIRST RESPONDERS

First responders can find intelligence products on a variety of classified and unclassified systems. Sensitive But Unclassified (SBU) systems include Law Enforcement Online (LEO) and the Homeland Secure Information Network (HSIN) on the Internet. First responders with the appropriate level of clearance and access can view classified information on NCTC CURRENT, the DHS Office of Intelligence and Analysis portal, and other sites on Secret-level systems, such as the FBI Network (FBINet), the Homeland Secure Data Network (HSDN), the Joint Deployable Intelligence Support System (JDISS), and the Secure Internet Protocol Router Network (SIPRNet).

THE TYPES OF PRODUCTS FIRST RESPONDERS WILL MOST LIKELY ENCOUNTER APPEAR BELOW:

- **Information reports** are typically messages that enable the timely dissemination of unevaluated intelligence within the IC and the law enforcement community.
- **Intelligence Assessments (IAs)** are finished intelligence products resulting from the intelligence analysis process. Assessments may address tactical, strategic, or technical intelligence requirements.
- **Intelligence Bulletins (IBs)** are finished intelligence products used to disseminate information of interest, such as significant developments and trends, to the intelligence and law enforcement communities in an article format.
- **Joint products** are intelligence assessments and bulletins produced in cooperation with other agencies (dual or multiple seals). When written jointly, these products may be formatted differently than the single-seal versions, depending on the format agreed to by participating agencies.
- **Threat Assessments (TAs) or Special Assessments (SAs)** provide in-depth analyses related to a specific event or body of threat reporting and may address nonterrorist threats to national security.

SPECIFIC PRODUCT LINES include digests, bulletins, and reference aids that cover counterterrorism, homeland security, and information related to weapons of mass destruction. Following are examples:

- **Alliance: Partnerships in Domestic Counterterrorism.** An NCTC, FBI, and DHS collaborative magazine that features Unclassified//For Official Use Only (U//FOUO) counterterrorism intelligence articles and resources for local, state, tribal, and territorial first responders, this product is available on NCTC CURRENT, HSIN, and LEO and in hardcopy from NCTC's Domestic Representatives.
- **Fire Line.** A one-page, DHS U//FOUO informational product issued jointly with FBI or as a triseal product with NCTC, this is intended to help the approximately 1 million state, local, tribal, and territorial fire, rescue, and emergency medical services first responders recognize and identify indicators of terrorism planning, support, and operations. Fire Lines potentially influence responder, mitigation, and safety operations and are available on HSIN and LEO.
- **First Responder Toolbox.** This ad hoc U//FOUO reference aid promotes counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private-sector officials in deterring, preventing, disrupting, and responding to terrorist attacks. First Responder Toolbox is available through HSIN and LEO, and select editions can be found on InfraGard and in the Domestic Security Alliance Council (DSAC) portals.

- **NCTC Counterterrorism Weekly (CT Weekly).** FOUO compilation of open-source information related to terrorism that may be of interest to federal, state, local, tribal, and territorial first responders and public safety personnel. The CT Weekly can be found on NCTC CURRENT, HSIN, and LEO.
- **NCTC CURRENT.** CURRENT articles are U//FOUO counterterrorism intelligence products published by NCTC and are available on HSIN and LEO.
- **Roll Call Release (RCR).** The DHS RCR, issued jointly with FBI or as a triseal product with NCTC, is a one-page, U//FOUO informational product written specifically for state, local, tribal, and territorial first responders and focused on a single topic. RCRs highlight emerging terrorist tactics, techniques, and procedures; terrorism trends; and potential indicators of suspicious activity that frontline law enforcement officers may encounter in the course of their official duties. RCRs are available on HSIN and LEO.



JOINT PARTNERSHIPS

“BY ITS NATURE INTELLIGENCE IS IMPERFECT (I.E., EVERYTHING CANNOT BE KNOWN, ANALYSIS IS VULNERABLE TO DECEPTION, AND INFORMATION IS OPEN TO ALTERNATIVE INTERPRETATIONS). THE BEST WAY TO AVOID THESE OBSTACLES AND ACHIEVE A HIGHER DEGREE OF FIDELITY IS TO CONSULT WITH, AND SOLICIT THE OPINIONS OF, OTHER ANALYSTS AND EXPERTS, PARTICULARLY IN EXTERNAL ORGANIZATIONS.”

23 OCTOBER 2013 EDITION OF JOINT PUB 2-0, JOINT INTELLIGENCE

JOINT PARTNERSHIPS

Federal, state, local, tribal, and territorial governments understand the benefits and value of working together and have established several programs to protect the U.S. within our borders. These programs include the Joint Terrorism Task Force (JTTF), National Joint Terrorism Task Force (NJTTF), and National Network of Fusion Centers. These programs take advantage of the broad experience, knowledge, and skills of personnel from a wide variety of fields, such as intelligence, law enforcement, fire services, and emergency services.

- **Domestic Security Alliance Council (DSAC):** DSAC, a strategic partnership among FBI, DHS, and the private sector, enhances communication and promotes the timely and bidirectional effective exchange of information that keeps the nation's critical infrastructure secure and resilient.
- **InfraGard** is a partnership between FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.
- **Joint Counterterrorism Assessment Team (JCAT):** The mission of JCAT is to improve information sharing and enhance public safety. JCAT collaborates with other members of the IC to research, produce, and disseminate counterterrorism intelligence products for federal, state, local, tribal, and territorial government agencies and the private sector and advocates for the counterterrorism intelligence requirements and needs of these partners throughout the IC.
- **Joint Terrorism Task Force (JTTF):** JTTFs serve as the coordinated “action arms” for federal, state, and local governments to investigate terrorist threats in specific U.S. geographic regions. FBI serves as the lead agency to oversee JTTFs. The benefits of a JTTF include the following:
 - » “One-stop shopping” for law enforcement information or investigation of suspected or real terrorist activities
 - » Use of a shared intelligence base
 - » Ability to prosecute cases in the jurisdiction that is most efficient and effective
 - » Task force member awareness of investigations within a jurisdiction and ability to assist in investigations in other jurisdictions
 - » Established relationships among agencies, investigators, and managers before a crisis occurs

The mission of the JTTF is to use the collective resources of the member agencies to prevent, preempt, deter, and investigate terrorist acts that affect U.S. interests; to disrupt and prevent terrorist acts; and to apprehend individuals who may commit or plan to commit such acts. To further this mission, the JTTF facilitates information sharing among JTTF members. More than 500 state and local agencies participate in JTTFs nationwide, and federal representation includes participants from the IC, DHS, and the Departments of Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and the Interior, among others.

- **National Joint Terrorism Task Force (NJTTF):** The mission of the NJTTF is to enhance communication, coordination, and cooperation among federal, state, and local government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, transportation, and homeland security communities by providing a point of fusion for terrorism intelligence and by supporting JTTFs throughout the country.

- » The FBI-led NJTTF was established in July 2002 to serve as a coordinating mechanism with FBI's partners.
- » Approximately 40 agencies are represented in the NJTTF, which has become a focal point for information sharing and management of large-scale projects that involve multiple partners.
- **Fusion centers:** A fusion center, run by the applicable state or local jurisdiction, exchanges information and intelligence, maximizes resources, streamlines operations, and improves the ability to disrupt, prevent, respond to, and recover from all threats by analyzing data from a variety of sources. A “collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing a center’s ability to detect, prevent, investigate, and respond to criminal and terrorist activity,” fusion centers focus primarily on the processes through which information is gathered, integrated, evaluated, analyzed, and disseminated.

State and major urban area fusion centers provide analysis and information-sharing capabilities that support the efforts of federal, state, and local law enforcement entities to prevent and investigate crime and terrorism. Fusion centers receive information from a variety of sources, including state and local tips and leads as well as federal information and intelligence. By “fusing” information from a wide variety of disciplines to conduct analysis, fusion centers generate products that are timely and relevant to their customers’ needs. This allows federal, state and local law enforcement to address immediate and emerging threat-related circumstances and events. It also supports risk-based, information-driven prevention, response, and consequence management.

- » Fusion centers are designed to involve every level and discipline of government, private-sector entities, and the public—although the level of involvement of some participants will vary.
- » Fusion centers are state and locally owned and operated. DHS has a statutory program to support fusion centers.

- **National Counterterrorism Center Domestic Representatives:** The NCTC Domestic Representative Program is the cornerstone for NCTC’s initiative to connect with various regional partners throughout the U.S. to facilitate the flow of information to and from NCTC. Located in several major cities across the country, NCTC Reps partner with regional IC organizations and state, local, tribal, and territorial counterterrorism officials by establishing professional relationships, providing tailored analytic briefs on threat and terrorism trends, and contributing to ongoing counterterrorism investigations. NCTC Reps also coordinate further support provided by NCTC, such as bringing additional expert analysts and prevention programming to the field.

What Is the Difference Between a JTTF and a Fusion Center?

JTTFs are FBI-sponsored, multijurisdictional task forces established specifically to conduct terrorism-related investigations, intelligence collection, and HUMINT source operations. **Fusion centers**, in contrast, are not investigative entities and do not focus solely on terrorism. These state and locally owned and operated information analysis centers analyze intelligence regarding a broad array of criminal and other activities related to homeland security. Fusion centers focus on trend and pattern analysis intended to help federal, state, and local law enforcement agencies mitigate emerging hazards, criminal problems, and other threats to the U.S.

SECTION THREE

REFERENCES

TERMINOLOGY

Terminology used in intelligence circles may seem straightforward at first glance, but the definitions often differ from conventional use. The following list of terms is not exhaustive but contains the terms likely to be encountered within intelligence material or while interacting with intelligence personnel. Although these terms may have other definitions, we selected these because they are the most relevant for first responders.

A

- actionable:** (1) information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process; the information may address strategic or tactical needs, support of U.S. negotiating teams, or actions dealing with such matters as international terrorism or narcotics; (2) intelligence and information with sufficient specificity and detail that explicit responses to prevent a crime or terrorist attack can be implemented
- access:** (1) the means, ability, or permission to approach, enter, or use a resource; (2) the basis for and ability of a HUMINT source to collect information against a specific subject or issue
- agent:** an individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence or counterintelligence purposes
- all-source intelligence:** intelligence information derived from any or all of the intelligence disciplines, including SIGINT, HUMINT, MASINT, OSINT, and GEINT
- analysis:** the process by which people transform information into intelligence; systematic examination of information to identify significant facts, make judgments, and draw conclusions

B

- basic intelligence:** intelligence on a subject that may be used as reference material for planning and evaluating subsequent information
- behavioral indicators of terrorism:** potential criminal or noncriminal activities requiring additional information during the vetting process or investigation, as well as defined criminal activity and potential terrorism nexus activity. When the activity involves behavior that may be lawful or is a constitutionally protected activity, the investigating law enforcement agency will carefully assess the information and gather as much information as possible before taking any action, including documenting and validating the information as terrorism-related and sharing it with other law enforcement agencies.
- behaviors:** observable actions

C

- case officer:** a professional employee of an intelligence organization who is responsible for providing direction for an agent operation
- clandestine activity:** any activity or operation sponsored or conducted by governmental departments or agencies with the intent to ensure secrecy or concealment (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)
- clandestine collection:** the acquisition of protected intelligence information in a way designed to protect the source and conceal the operation, the identity of operators and sources, and the actual methodologies employed (DoDI S-5240.17, CI collection, 12 Jan 2009)
- classification:** the determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made; the designation is normally termed a

- security classification and includes Confidential, Secret, and Top Secret
- collation (of information):** a review of collected and evaluated information to determine its substantive applicability to a case or problem and the placement of useful information into a form or system that permits easy and rapid access and retrieval
- collection (of information):** the identification, location, and recording or storing of information—typically from an original source and using both human and technological means—for input into the intelligence cycle to meet a defined tactical or strategic intelligence goal
- collection plan:** the preliminary step toward completing an assessment of intelligence requirements to determine what type of information needs to be collected, alternatives for how to collect the information, and a timeline for collecting the information
- communications intelligence (COMINT):** the capture of information, either encrypted or in “plaintext,” exchanged between intelligence targets or transmitted by a known or suspected intelligence target for tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, or analyzing the substantive meaning of the communication; a subdiscipline of SIGINT
- conclusion:** a definitive statement about a suspect, action, or state of nature based on analysis of information
- Confidential:** a security classification designating information that, if made public, could be expected to cause damage to national security
- consumer:** an authorized person who uses intelligence or intelligence information directly in the decisionmaking process or to produce other intelligence
- coordination:** (1) the process by which producers obtain the views of other producers on the adequacy of a specific draft assessment, estimate, or report; it is intended to increase a product’s accuracy, clarify its judgments, and resolve or sharpen statements of disagreement on major contentious issues; (2) the process of seeking concurrence from one or more groups, organizations, or agencies regarding a proposal or an activity for which they share some responsibility and that may result in contributions, concurrences, or dissents
- counterintelligence:** information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities
- counterterrorism:** (1) the practices, tactics, techniques, and strategies adopted to prevent or respond to terrorist threats or acts, both real and imputed; (2) a strategy intended to prevent or counter terrorism
- covert:** a method of conducting operations that hides the true intent, affiliation, or relationship of its participants; differs from clandestine in that covert activity conceals the identity of the sponsor, whereas clandestine conceals the identity of the operation (National HUMINT Glossary)
- covert action:** an activity or activities undertaken by the U.S. Government to influence political, economic, or military conditions abroad where the U.S. Government’s role should not be apparent or acknowledged publicly; does not include activities conducted primarily to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of U.S. Government programs, or administrative activities (Section 503e, National Security Act of 1947 [50 USC §413b])

critical infrastructure information: information related to the security of critical infrastructure or protected systems: (1) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the U.S., or threatens public health or safety; (2) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk management planning, or risk audit; or (3) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation (Homeland Security Act of 2002, as amended)

cryptanalysis: the process of deciphering encrypted communications of an intelligence target

cryptography: the creation of a communications code or encryption system for communication transmission with the intent of precluding the consumption and interpretation of one's own messages

cryptology: the study of communications encryption methods that deals with the development of "codes" and the "scrambling" of communications to prevent interception by an unauthorized or unintended party

current intelligence: intelligence of all types and forms of immediate interest to users; it may be disseminated without complete evaluation, interpretation, analysis, or integration

D

deconfliction: the process or system used to determine whether multiple law enforcement agencies are investigating the same person or crime and that provides notification to each agency involved of the shared interest in the case, as well as providing contact information; an information- and intelligence-sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of an investigation

deductive logic: the reasoning process of using information to arrive at conclusions

deployment: the short-term assignment of personnel to address specific national security-related problems or demands

dissemination (of intelligence): the timely distribution of intelligence products to consumers in a suitable form (oral, written, or graphic)

downgrade: the process of editing or otherwise altering intelligence materials, information, reports, or other products to conceal and protect intelligence sources, methods, capabilities, analytic procedures, or privileged information in order to permit wider distribution (see *sanitization*)

E

electronic intelligence (ELINT): (1) information derived primarily from electronic signals that do not contain speech or text (which are considered COMINT); (2) information obtained for intelligence purposes from the intercept of electromagnetic non-communications transmissions by other

than the intended recipient; the most common sources are radar signals; a subdiscipline of SIGINT

essential elements of information: items of intelligence information vital for timely decisions and for enhancement of operations that relate to foreign powers, forces, targets, or physical environments (see *priority intelligence requirement*)

estimate: (1) analysis of a situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and prospective results of various actions that might be taken; (2) an appraisal of the capabilities, vulnerabilities, and potential courses of action a foreign nation or combination of nations may take in reaction to a specific national plan, policy, decision, or contemplated course of action; (3) analysis of an actual or contemplated clandestine operation in relation to the situation in which it is or would be conducted to identify and appraise such factors as available and needed assets and potential obstacles, accomplishments, and consequences (see *National Intelligence Estimate*)

estimative intelligence: a category of intelligence that attempts to predict probable future foreign courses of action and developments and their implications for U.S. interests; it may or may not be coordinated and may be national or departmental intelligence

evaluation: an appraisal of the worth of an intelligence activity, information, or product in terms of its contribution to a specific goal; all information collected for the intelligence cycle is reviewed for its quality with an assessment of the validity and reliability of the information

exploitation: the process of obtaining intelligence information from any source and taking advantage of it for intelligence purposes

F

Field Intelligence Group (FIG): the centralized intelligence component in an FBI field office responsible for the management, execution, and coordination of intelligence functions within the region

finished intelligence: an intelligence product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information

foreign instrumentation signals intelligence (FISINT): information derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems including, but not limited to, telemetry, beaconry, electronic interrogators, and video data links; a subdiscipline of SIGINT

Foreign Intelligence Surveillance Act (FISA): the FISA Act of 1978 prescribes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between or among "foreign powers" on territory under U.S. control; codified in 50 U.S.C. §§1801-1811, 1821-29, 1841-46, and 1861-62; amended by the USA PATRIOT Act of 2001, primarily to include terrorism by groups that are not specifically backed by a foreign government

For Official Use Only (FOUO): a dissemination control marking used to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely affect a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest

Freedom of Information Act (FOIA): the Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to gain access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions or three exclusions

fusion center: a collaborative effort of two or more agencies that provide resources, expertise, and information with the goal of maximizing the ability to detect, prevent, investigate, and respond to criminal and terrorism activity; recognized as a valuable information-sharing resource, state and major urban area fusion centers are the focus, but not exclusive points, within the state and local environment for the receipt and sharing of terrorism information, homeland security information, and law enforcement information related to terrorism

G

geospatial: describes any data containing coordinates defining a location on the Earth's surface

geospatial intelligence (GEOINT): intelligence derived from the exploitation of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth

granularity: considers the specific details and pieces of information, including nuances and situational inferences, that constitute the elements on which intelligence is developed through analysis

H

high side: a colloquial term for classified government computer systems

hypothesis: an interim conclusion regarding persons, events, or commodities that is formed based on the accumulation and analysis of intelligence information; must be proven or disproven by further investigation and analysis

I

imagery intelligence (IMINT): includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media; can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics

indications and warning (I&W): intelligence activities intended to detect and report time-sensitive intelligence information on developments that could involve a threat to U.S. or allied military, political, or economic interests, or to U.S. citizens abroad

indicators: generally defined and observable actions that, based on analysis of past known behaviors and characteristics, collectively suggest that a person may be committing, may be preparing to commit, or has committed an unlawful act

inductive logic: the reasoning process of using diverse pieces of specific information to infer (from the information) a broader meaning through the course of hypothesis development

inference development: the creation of a probabilistic conclusion, estimate, or prediction related to an intelligence target by using inductive or deductive logic in the analysis of raw information

informant: an individual not affiliated with a law enforcement agency who provides information about criminal behavior; may be a community member, a businessperson, or a criminal informant who seeks to protect himself or herself from prosecution or provide the information in exchange for payment

information: pieces of raw, unanalyzed data that identify persons, evidence, or events or illustrate processes that indicate the incidence of an event or evidence of an event

Information Sharing Environment-Suspicious Activity Reporting (ISE-SAR): As defined by ISE-SAR Functional Standard 1.5.5; is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE

Information Sharing Environment (ISE): in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004, Section 1016, and Executive Order 13388, entitled "Further Strengthening the Sharing of Terrorism Information to Protect Americans," the ISE is defined as the combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of all federal Executive Branch entities to facilitate terrorism information sharing, access, and collaboration among users in order to combat terrorism more effectively; provides links to state, local, tribal, and territorial government agencies and the private sector to ensure effective sharing of information among all relevant entities; designed to meet the dual imperatives of sharing critical information and protecting privacy and civil liberties

information-sharing system: an integrated and secure methodology, whether computerized or manual, designed to efficiently and effectively distribute critical information

intelligence analyst: a professional intelligence officer responsible for performing, coordinating, or supervising the collection, analysis, and dissemination of intelligence

intelligence activity: a generic term used to encompass any or all of the efforts undertaken by intelligence organizations, including collection, analysis, production, dissemination, and covert or clandestine activities

intelligence agency: a component organization of the Intelligence Community

Intelligence Assessment (IA): a longer, often detailed intelligence product; encompasses most analytic studies dealing with subjects of policy significance

Intelligence Bulletin (IB): a shorter, often less detailed intelligence product that focuses on a particular topic or incident

Intelligence Community (IC): a federation of Executive Branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of U.S. national security; these organizations are (in alphabetical order) Air Force Intelligence, Army Intelligence, the Central Intelligence Agency, Coast Guard Intelligence, the Defense Intelligence Agency, the Department of Energy, the Department of Homeland Security, the Department of State, the Department of the Treasury, the Director of National Intelligence, the Drug Enforcement Administration, the Federal Bureau of Investigation, Marine Corps Intelligence, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency, and Navy Intelligence

intelligence cycle: the steps by which information is converted into intelligence and made available to users; has been described as including five steps: planning and direction, collection, processing, production, and dissemination; evaluation, although generally assumed, is a sixth step in the cycle considered essential

Intelligence Estimate: analysis of a situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and the prospective results of the various actions that might be taken (see *National Intelligence Estimate*)

intelligence information: unevaluated material that may be used in the production of intelligence

intelligence-led policing: the dynamic use of intelligence to guide operational law enforcement activities to targets, commodities, or threats for both tactical responses and strategic decisionmaking for resource allocation or strategic responses

intelligence mission: the role that the intelligence function of an agency fulfills in support of the overall mission of the agency; specifies in general language what the function is intended to accomplish

intelligence needs: intelligence requirements not being addressed in current intelligence activities to support customers and missions

intelligence officer: a professional employee of an intelligence organization engaged in intelligence activities

intelligence products: reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process

intelligence requirement: any subject, general or specific, for which there is a need to collect intelligence information or to produce intelligence

J

Joint Terrorism Task Force (JTTF): coordinated “action arm” for federal, state, and local government response to terrorist threats in specific U.S. geographic regions; FBI is the lead agency that oversees JTTFs

K

known or suspected terrorist (KST): individuals known or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to terrorism

L

Law Enforcement Sensitive (LES): unclassified information typically originated by FBI that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence, and the integrity of pretrial investigative reports

low side: a colloquial term for a non–Top Secret computer system; can be used to refer to Unclassified or Secret-level systems

M

measurement and signature intelligence (MASINT): technically derived intelligence data other than imagery and SIGINT; results in intelligence

that locates, identifies, or describes distinctive characteristics of targets; employs a broad group of disciplines, including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences

methods: these are the methodologies (that is, electronic surveillance or undercover operations) of how critical information is obtained and recorded

N

National Counterterrorism Center (NCTC): serves as the primary organization in the U.S. Government for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the U.S. Government (except purely domestic terrorism); serves as the central and shared knowledge bank on terrorism information; provides all-source intelligence support to government-wide counterterrorism activities; establishes the information technology systems and architectures within NCTC and between NCTC and other agencies that enable access to as well as integration, dissemination, and use of terrorism information

National Intelligence Council (NIC): the IC’s center for midterm and long-term strategic thinking; primary functions are to support the Director of National Intelligence, provide a focal point for policymakers to task the IC to answer their questions, reach out to nongovernment experts in academia and the private sector to broaden the IC’s perspective, contribute to the IC’s effort to allocate its resources to policymakers’ changing needs, and lead the IC’s effort to produce National Intelligence Estimates and other NIC products

National Intelligence Estimate (NIE): produced by the NIC, express the coordinated judgments of the IC, and thus represent the most authoritative assessment of the Director of National Intelligence with respect to a particular national security issue; contain the coordinated judgments of the IC regarding the probable course of future events

national security: measures adopted by the government of a nation in order to ensure the safety of its citizens, guard against attack, and prevent disclosure of sensitive or classified information that might threaten or embarrass said nation

national security intelligence: the collection and analysis of information about the relationship and equilibrium of the U.S. with foreign powers, organizations, and persons regarding political and economic factors, as well as the maintenance of the U.S.’s sovereign principles

National Terrorism Advisory System (NTAS): more effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports, and other transportation hubs, as well as the private sector; recognizes that Americans all share responsibility for the nation’s security and should always be aware of the heightened risk of terrorist attacks in the U.S. and what they should do

network: a structure of interconnecting components or persons designed to communicate with each other and perform a function or functions as a unit in a specified manner

No Fly (TSA): an individual not permitted to board commercial flights because of terrorism concerns

No-Fly list: a list created and maintained by the U.S. Government to keep known or suspected terrorists from boarding and flying on commercial flights

O

open source: information of potential intelligence value that is available to the general public and can be used to enhance intelligence analysis and reporting

open-source intelligence (OSINT): publicly available information appearing in print or electronic form, including radio, television, newspapers, journals, the Internet, commercial databases, videos, graphics, and drawings used to enhance intelligence analysis and reporting

operational intelligence: (1) intelligence required for planning and executing operations; (2) information on an active or potential target, such as a group or individual, relevant premises, contact points, and methods of communication, that is evaluated and systematically organized; the process is developmental in nature wherein there are sufficient articulated reasons to suspect nefarious activity

operations security: a systematic, proven process by which a government, organization, or individual can identify, control, and protect generally unclassified information about an operation or activity and thus deny or mitigate an adversary's or competitor's ability to compromise or interrupt said operation or activity

P

personally identifiable information: (1) as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual; (2) any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual; *individual* includes, but is not limited to, U.S. citizens, legal permanent residents, and visitors to the U.S.; *information* includes any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, and so on, including any other personal information that is linked or linkable to an individual

plus one: (1) one additional something (for example, person or data element); (2) an individual's name plus an additional data element (that is, date of birth, social security number, passport number); typically used in reference to information, beyond an individual's name, required to confirm an individual's identity

policy: the principles and values that guide the performance of a duty; not a statement of what must be done in a particular situation but a statement of guiding principles that should be followed in activities directed toward the attainment of goals

prediction: the projection of future actions or changes in trends based on the analysis of information depicting historical trends

priority intelligence requirement: a prioritized informational need critical to mission success

privacy (information): the assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by anyone who has

access to such information, with use of such information to be strictly limited to circumstances in which legal process permits

privacy (personal): the assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual—including his or her communications, associations, and transactions—will be adhered to by anyone who has access to such information, with use of such information to be strictly limited to circumstances in which legal process authorizes surveillance and investigation

Privacy Act: the Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies; requires that agencies give the public notice of their systems of records by publication in the Federal Register; prohibits disclosure of information from a system of records absent written consent from the subject individual, unless the disclosure is pursuant to one of 12 statutory exceptions; also provides individuals with a means by which to seek access to and amend their records and sets forth various agency recordkeeping requirements

private-sector partners: as used in the ISE Implementation Plan, private-sector partners include vendors, owners, and operators of products and infrastructures participating in the ISE

Protected Critical Infrastructure Information (PCII) Program: enhances information sharing between the private sector and the government; DHS and other federal, state, and local analysts use PCII to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures

Q

qualitative (methods): research methods that collect and analyze information described in narrative or rhetorical form, with conclusions drawn based on the cumulative interpreted meaning of that information

quantitative (methods): research methods that collect and analyze information that can be counted or placed on a scale of measurement and statistically analyzed

R

raw data: bits of data collected that individually convey little or no useful information and must be collated, aggregated, or interpreted to provide meaningful information

raw intelligence: a colloquial term meaning collected intelligence information that has not yet been vetted, validated, or analyzed

Regional Information Sharing Systems (RISS): composed of six regional intelligence centers that provide secure communications, information-sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats to federal, state, local, tribal, and territorial member law enforcement agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England

requirements (intelligence): the details of what a customer needs from intelligence

responsibility: reflects how the authority of a unit or individual will be used and determines whether goals have been accomplished and the mission

fulfilled in a manner consistent with the defined limits of authority
risk: the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

risk assessment: analysis of a target, illegal commodity, or victim to identify the probability of being attacked or compromised and to analyze vulnerabilities; generally includes preventative steps to be taken to lessen the risk

S

sanitization: the process of editing or otherwise altering intelligence materials, information, reports, or other products to conceal and protect intelligence sources, methods, capabilities, analytic procedures, or privileged information to permit wider dissemination

Secret: information that, if made public, could be expected to cause serious damage to national security

Selectee (TSA): an individual who must undergo additional security screening before being permitted to board a commercial aircraft

Sensitive But Unclassified (SBU): information that has not been classified by a federal law enforcement agency that pertains to significant law enforcement cases under investigation and to criminal intelligence reports and for which dissemination is permitted to only those persons necessary to further the investigation or to prevent a crime or terrorist act

Sensitive Compartmented Information (SCI): classified information concerning or derived from intelligence sources, methods, or analytic processes that must be handled within formal access control systems established by the Director of National Intelligence

Sensitive Compartmented Information facility (SCIF): an accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, or processed

Sensitive Security Information (SSI): is a specific category of sensitive but unclassified information that is governed by federal law. SSI is information obtained or developed which, if released publicly, would be detrimental to transportation security. SSI is not classified national security information and is not subject to the handling requirements governing such information, but is subject to the handling procedures required by the SSI Federal Regulation (49 CFR Part 1520). Unauthorized disclosure of SSI may result in civil penalties and other enforcement or corrective actions.

signals intelligence (SIGINT): intelligence derived from signals intercepts comprising, individually or in combination, all COMINT, ELINT, and FISINT

source: a book, statement, person, or other entity supplying information; from a HUMINT perspective, sources are persons who collect or possess critical information needed for intelligence analysis

Suspicious Activity Report (SAR): per the ISE-SAR Functional Standard 1.5.5, official documentation of "observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity"

system of records: in accordance with the Privacy Act of 1974, a system of records is a group of any records under the control of any agency from which information can be retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual; the Privacy Act requires each agency to publish notice of its systems of records, generally referred to as a System of Records Notice (SORN) in the Federal Register

T

tactical intelligence: information regarding a specific event that can be used immediately by operational units to further investigations, plan tactical operations, support preparedness and response or recovery operations, and provide for first responder safety

target: (1) any person, organization, group, crime or criminal series, or commodity subject to investigation and intelligence analysis; (2) an individual, operation, or activity that an adversary has determined possesses information that might prove useful in attaining his or her objective

target profile: a person-specific profile that contains sufficient detail to initiate a targeting operation or support an ongoing operation against that individual or a network of such individuals

targeting: the identification of incidents, trends, and patterns with discernable characteristics that makes collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those responsible

tear line: intelligence information that has been sanitized (by removal of sources and methods) so it may be disseminated at a lower classification

tear-line report: a report containing classified intelligence or information prepared so that data relating to intelligence sources and methods can be easily removed to protect sources and methods from disclosure; typically, the information below the "tear line" can be released as SBU

terrorism: Title 22 of the U.S. Code, Section 2656f(d) defines terrorism as premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience

Terrorist Identities Dataamart Environment (TIDE): a consolidated repository of information on international terrorist identities that is the authoritative database supporting the Terrorist Screening Center and the U.S. Government's watchlisting system

terrorism information: all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to (1) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (2) threats posed by such groups or individuals to the U.S., U.S. persons, or U.S. interests, or to those of other nations; (3) communications of or by such groups or individuals; or (4) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; includes weapons of mass destruction information

Terrorist Screening Center (TSC): established in support of Homeland Security Presidential Directive 6 (HSPD-6), dated 16 September 2003, to consolidate the U.S. Government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes; maintains the U.S. Government's consolidated and integrated terrorist watchlist, known as the Terrorist Screening Database

Terrorist Screening Database (TSDB): contains the consolidated and integrated terrorist watchlist maintained by FBI's TSC; the No-Fly and Selectee Lists are components

third-agency rule: an agreement wherein a source agency releases information under the condition that the receiving agency does not release the information to any other agency—that is, a third agency

threat: (1) a source of unacceptable risk; (2) the capability of an adversary, coupled with his or her intentions to undertake actions detrimental to the success of program activities or operations

threat assessment: appraisal of the threat that an activity or group poses to a jurisdiction, either at present or in the future, that may recommend ways to lessen the threat; the assessment focuses on opportunity, capability, and willingness to fulfill the threat

Top Secret: information that, if made public, could be expected to cause exceptionally grave damage to national security

Y — Z —

U —

unauthorized disclosure: a communication or physical transfer, usually of SBU or classified information, to an unauthorized recipient

Unclassified: information not subject to a security classification; that is, information not Confidential, Secret, or Top Secret; although unclassified information is not subject to a security classification, there may still be limits on disclosure

Urban Areas Security Initiative (UASI): a grants program that focuses on enhancing regional preparedness in major metropolitan areas

V —

validity: information that has some foundation or is based on truth; asks the question, "Does the information actually represent what we believe it represents?"

variable: any characteristic on which individuals, groups, items, or incidents differ

vet: (1) to subject a proposal, work product, or concept to an appraisal by command personnel or subject matter experts to ascertain the product's accuracy, consistency with philosophy, or feasibility before proceeding; (2) to subject information or sources to careful examination or scrutiny to determine suitability

vulnerability: a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard

vulnerability assessment: an assessment of possible terrorist targets within a jurisdiction integrated with an assessment of the targets' weaknesses, likelihood of being attacked, and ability to withstand an attack

W —

warning: to notify in advance of possible harm or victimization as a result of information and intelligence gained concerning the probability of a crime or terrorist attack

X —

ACRONYMS AND ABBREVIATIONS

The Intelligence Community makes extensive use of acronyms and abbreviations in intelligence reporting, presentations, and conversation—many are unique to this community, and some have multiple meanings. They are so frequently used, that sometimes an acronym or abbreviation may be well known and understood; however, the user could not tell you what the letters mean. The following list, while not exhaustive, contains acronyms and abbreviations that are likely to be encountered by first responders reading intelligence material or interacting with intelligence personnel.

A

AAA: Asbat al-Ansar
AAB: 'Abdallah Azzam Brigades
AAD: Ansar al-Din
AAI: Ansar al-Islam
AAMB: Al-Aqsa Martyrs Brigade
AAR: After-Action Report
ACIC: Army Counterintelligence Center
AFIS: Automated Fingerprint Identification System
AFOSI: Air Force Office of Special Investigations
AKA: also known as
AMCIT: American citizen
AMEMB: American Embassy
ANO: Abu Nidal Organization
ANW: alerts, notifications, and warnings
AOI: Army of Islam
AQ: al-Qa'ida
AQAP: al-Qa'ida in the Arabian Peninsula
AQIM: al-Qa'ida in the Lands of the Islamic Maghreb (formerly Salafist Group for Preaching and Combat [GSPC])
ASG: Abu Sayyaf Group
ATF: Bureau of Alcohol, Tobacco, and Firearms
AUC: United Self-Defense Forces of Colombia
AUM: Aum Shinrikyo
AUSA: Assistant U.S. Attorney

B

BPA: Border Patrol agent
BW: biological warfare

C

C: Confidential
CBP: U.S. Customs and Border Protection (DHS)
CBR: chemical, biological, and radiological
CBRN: chemical, biological, radiological, and nuclear
CBRNE: chemical, biological, radiological, nuclear, and explosives
CBT: computer-based training
CBW: chemical and biological warfare
CDD: chemical dispersion device
CI: counterintelligence
CI poly: counterintelligence polygraph
CIA: Central Intelligence Agency
CIR: Central Intelligence Report
CIR: Counterintelligence Report
CIR: Current Intelligence Report
CIRA: Continuity Irish Republican Army
CLASS: Consular Lookout and Support System
COI: Community of Interest
COMINT: communications intelligence
COMSEC: communications security

CONOPS: concept of operations
CONUS: continental U.S.
COOP: continuity of operations
CPP/NPA: Communist Party of the Philippines/New People's Army
CT: counterterrorism

D

D/CIA: Director, Central Intelligence Agency (formerly DCI)
D&D: denial and deception
DEA: Drug Enforcement Administration
DCTC: Defense Combating Terrorism Center
DHKP/C: Revolutionary People's Liberation Army/Front
DHS: Department of Homeland Security
DI: Directorate of Intelligence
DIA: Defense Intelligence Agency
DISES: Defense Intelligence Senior Executive Service
DISL: Defense Intelligence Senior Level
DNI: Director of National Intelligence
DOB: date of birth
DOD: Department of Defense
DOE: Department of Energy
DOS: Department of State
DPOB: date and place of birth
DSAC: Domestic Security Alliance Council
DSS: Diplomatic Security Service
DT: domestic terrorism

E

EEl: essential element of information (now priority intelligence requirement [PIR])
EIF: entry into force
ELINT: electronic intelligence
ELN: National Liberation Army
EO: executive order
EPA: Environmental Protection Agency
ETA: estimated time of arrival
ETA: Basque Fatherland and Liberty
EWI: entry without inspection

F

FAA: Federal Aviation Administration
FAM: Federal Air Marshal
FARC: Revolutionary Armed Forces of Colombia
FBI: Federal Bureau of Investigation
FEMA: Federal Emergency Management Agency
FGI: Foreign Government Information
FIG: Field Intelligence Group (FBI)
FIR: Field Information Report
FIS: foreign intelligence service
FISA: Foreign Intelligence Surveillance Act
FISINT: foreign instrumentation signals intelligence

FNU: first name unknown
FPO: Federal Protective Service Officer
FOIA: Freedom of Information Act
FOUO: For Official Use Only
FPS: Federal Protective Service
FPU: Force Protective Unit
FSLTTP: federal, state, local, tribal, territorial, and private sector

G

GEOINT: geospatial intelligence
GS: General Schedule

H

HCS: Human Control System
HIR: Homeland Information Report
HQN: Haqqani Network
HSC: Homeland Security Council
HSDN: Homeland Secure Data Network
HSIN: Homeland Security Information Network (DHS Internet portal)
HSIN-I: Homeland Security Information Network—Intelligence (DHS Internet portal)
HS SLCI: Homeland Security State and Local Community of Interest
HUJI-B: Harakat ul-Jihad-i-Islami/Bangladesh
HUM: Harakat ul-Mujahidin
HUMINT: human intelligence

I

I&A: Office of Intelligence and Analysis (DHS)
I&W: indications and warning
IA: Intelligence Assessment
IA: intelligence analyst
IAEA: International Atomic Energy Agency
IBIS: Interagency Border Inspection System
IC: Intelligence Community
ICCD: improvised chemical dispersion device
ICD: improvised chemical device
ICD: Intelligence Community Directive (replaces Director of Central Intelligence Directives or DCIDs)
ICE: U.S. Immigration and Customs Enforcement (DHS)
IDENT: Automated Biometric Fingerprint Identification System
IED: improvised explosive device
IG: al-Gama'at al-Islamiyya (Islamic Group, IG)
IG: Inspector General
IICT: Interagency Intelligence Committee on Terrorism (NCTC)
IIR: Intelligence Information Report
IJU: Islamic Jihad Union
IM: Indian Mujahideen
IMINT: imagery intelligence
IMU: Islamic Movement of Uzbekistan
INA: Immigration and Nationality Act

IND: improvised nuclear device
INFOSEC: information security
INR: Bureau of Intelligence and Research (Department of State)
INTERPOL: International Police
IRT: incident response team
IRTPA: Intelligence Reform and Terrorism Prevention Act of 2004
ISC: Information Sharing Council
ISE: Information Sharing Environment
ISE-SAR: Information Sharing Environment-Suspicious Activity Report
ISIL: Islamic State of Iraq and the Levant (formerly al-Qa'ida in Iraq; also referred to as Islamic State of Iraq and Syria [ISIS])
IT: international terrorism

J

JAT: Jemaah Anshorut Tauhid
JCAT: Joint Counterterrorism Assessment Team
JCS: Joint Chiefs of Staff
JEM: Jaish-e-Mohammad
Ji: Jemaah Islamiyah
JRIES: Joint Regional Information Exchange System
JSA: Joint Special Assessment
JTF: Joint Task Force
JTTF: Joint Terrorism Task Force
JWICS: Joint Worldwide Intelligence Communication System

K

KACH: Kahane Chai
KH: Kata'ib Hizballah
KST: known or suspected terrorist

L

LAN: local area network
LEA: law enforcement agency
LEEP: Law Enforcement Enterprise Portal
LEO: law enforcement officer
LEO: Law Enforcement Online (FBI SBU Web portal)
LES: Law Enforcement Sensitive
LIFG: Libyan Islamic Fighting Group
LJ: Lashkar-e-Jhangvi
LNU: last name unknown
LPR: Lawful Permanent Resident
LT: Lashkar-e-Tayyiba
LTTE: Liberation Tigers of Tamil Eelam

M

MANPADS: man-portable air defense system
MASINT: measurement and signature intelligence
MEK: Mujahedin-e Khalq Organization

MI: military intelligence
MOA: memorandum of agreement
MOU: memorandum of understanding
MSC: Mujahidin Shura Council in the Environs of Jerusalem

N

NAIS: National Automated Immigration Lookout System
NCIC: National Crime Information Center
NCIS: Naval Criminal Investigative Service
NCIX: National Counterintelligence Executive
NCPC: National Counterproliferation Center
NCR: national capital region
NCTC: National Counterterrorism Center
NFI: no further information
NFTR: nothing further to report
NGA: National Geospatial-Intelligence Agency
NIC: National Intelligence Council
NIE: National Intelligence Estimate
NIMA: National Imagery and Mapping Agency (now NGA)
NIP: National Intelligence Program
NIPF: National Intelligence Priorities Framework
NJTTF: National Joint Terrorism Task Force
NLETS: National Law Enforcement Telecommunication System
NOC: National Operations Center (DHS)
NOFORN: Not Releasable to Foreign Nationals
NOIWON: National Operations and Intelligence Watch Officers Network
NRO: National Reconnaissance Office
NSA: National Security Agency
NSC: National Security Council
NSEERS: National Security Entry-Exit Registration System
NSI: Nationwide Suspicious Activity Reporting Initiative
NSIS: National Strategy for Information Sharing
NSTL: National Security Threat List
NSTR: nothing significant to report
NSTS: National Secure Telephone System
NTAS: National Terrorism Advisory System
NTM: National Technical Means
NTR: nothing to report

O

OCONUS: outside the continental U.S.
ODNI: Office of the Director of National Intelligence
OPSEC: operations security
ORCON: Originator Controlled Dissemination
OSC: Open Source Center
OSINT: open-source intelligence
OSIS: Open Source Information System

P

PCII: protected critical infrastructure information
PFLP: Popular Front for the Liberation of Palestine

PFLP-GC: PFLP—General Command
PII: personally identifiable information
PIJ: Palestine Islamic Jihad
PIR: priority intelligence requirement (formerly essential element of information [EEI])
PKK: Kurdistan Workers' Party (Kongra-Gel or Kurdistan People's Congress)
PLF: Palestine Liberation Front
PM-ISE: Program Manager—Information Sharing Environment (DNI)
PM: production management
PNR: passenger name record
POB: place of birth
POC: point of contact
POE: port of entry
PPN: passport number
PSA: Protective Security Advisor (DHS)

Q

R

RDD: radiation dispersal device
RFI: request for information
RFP: request for proposal
RIRA: Real Irish Republican Army
RISS: Regional Information Sharing System
RISSNet: Regional Information Sharing System Network
RO: Reporting Officer or Reports Officer
RS: Revolutionary Struggle
RSO: Regional Security Office

S

S: Secret
S&T: science and technology
S&L: state and local
SA: situational awareness
SA: Special Assessment
SAP: special access program
SAR: Suspicious Activity Report
SBI: special background investigation
SBU: Sensitive But Unclassified
SCI: Sensitive Compartmented Information
SCIF: Sensitive Compartmented Information Facility
SEG: Special Events Group
SES: Senior Executive Service
SETA: Special Events Threat Assessment
SEVIS: Student Exchange Visitor Information System
SI: Sensitive Information
SI: Special Intelligence
SIA: Supervisory Intelligence Analyst
SIO: Supervisory Intelligence Officer
SIOC: Strategic Information and Operations Center (FBI)
SIPRNET: Secret Internet Protocol Routed Network

SIS: Senior Intelligence Service
SL: Shining Path
SLAM: SIOC Law Enforcement Alert Messaging System
SLTT: state, local, tribal, and territorial
SLTTP: state, local, tribal, territorial, and private sector
SME: subject matter expert
SNIS: Senior National Intelligence Service
SOP: standard operating procedure
SPII: sensitive personally identifiable information
SSI: sensitive security information
SSO: Special Security Officer
STE: secure telephone
STU III: Secure Telephone Unit III
SVTC: secure video teleconference

T

TA: Threat Analysis
TA: Threat Assessment
TD: Teletype Dissemination
TDX: Teletype Dissemination Sensitive
TDY: temporary duty
TECS: Treasury Enforcement Communications System
TIDE: Terrorist Identities Datamart Environment
TS: Top Secret
TSA: Transportation Security Administration
TSANOF: TSA No-Fly List
TSASEL: TSA Selectee List
TSC: Terrorist Screening Center
TSDB: Terrorist Screening Database
TSO: Transportation Security Officer
TSOC: Transportation Security Operations Center
TS//SCI: Top Secret//Sensitive Compartmented Information
TTP: tactics, techniques, and procedures
TTP: Tehrik-e Taliban Pakistan

U

U: Unclassified
UASI: Urban Areas Security Initiative (DHS grants program)
UBL: Usama Bin Ladin
U//FOUO: Unclassified//For Official Use Only
UI: unidentified
UNC: Unclassified
UNCLASS: Unclassified
UNK: unknown
USA: U.S. Attorney
USC: U.S. citizen
USCG: U.S. Coast Guard
USCIS: U.S. Citizenship and Immigration Services (DHS)
USDI: Undersecretary of Defense for Intelligence
USEMB: U.S. Embassy
USIC: U.S. Intelligence Community
USPER: U.S. person

V

VBIED: vehicle-borne improvised explosive device
VGTOF: Violent Gang and Terrorist Organization File
VTC: video teleconference
VWP: Visa Waiver Program

W

WMD: weapons of mass destruction

X

Y

Z

#

17N: Revolutionary Organization 17 November

DIGITAL FORMAT

This document can also be found in digital form at <https://hsin.dhs.gov> , <https://www.cjis.gov>, and <http://www.nctc.gov>.

