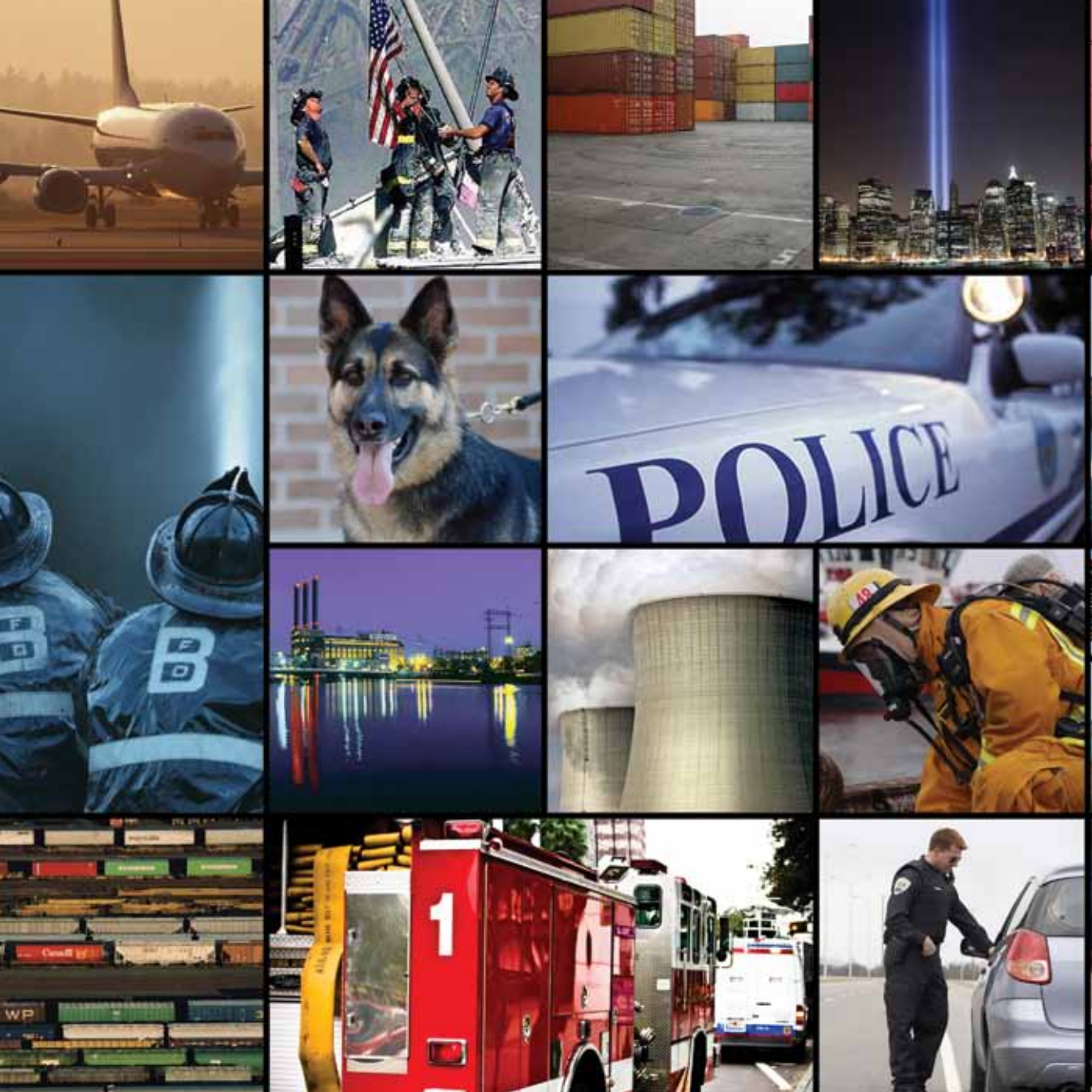
ITACG

Interagency Threat Assessment and Coordination Group

INTELLIGENCE GUIDE FOR FIRST RESPONDERS

2ND EDITION | MARCH 2011


POLICE

ITACG

Interagency Threat Assessment and Coordination Group

INTELLIGENCE GUIDE

FOR FIRST RESPONDERS

2nd Edition | March 2011

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.

This Handbook was coordinated through the Office of the Director of National Intelligence (ODNI), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC).

"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."

Exuctive Order 12333

INTRODUCTION

This Interagency Threat Assessment and Coordination Group (ITACG) ***Intelligence Guide for First Responders*** is designed to assist first responders in accessing and understanding Federal intelligence reporting and to encourage the sharing of information. The information in this guide was derived, compiled, and adapted from existing unclassified Intelligence Community and open-source references.

The ITACG consists of state, local, and tribal first responders from around the United States and federal intelligence analysts from the Department of Homeland Security, Federal Bureau of Investigation, and National Counterterrorism Center working to enhance the sharing of federal information on counterterrorism, homeland security, and weapons of mass destruction with state, local, and tribal consumers of intelligence.

Current and former state, local, and tribal members of the ITACG Detail as of February 2011: Abington Police Department, PA; Arlington Police Department, TX; Aurora Police Department, CO; Boston Police Department; Fairfax County Fire and Rescue Department, VA; Florida Department of Health; Hennepin County Sheriff's Office, MN; Illinois State Police (2008-2009); Indiana State Police; Las Vegas Metropolitan Police Department (2008-2009); Little River Band of Ottawa Indians Tribal Police Department, MI (2010); Metropolitan Police Department, Washington, DC (2008-2009); Nebraska Department of Health and Human Services (2009-2010); New Jersey State Police (2008-2010); Oakland County Sheriff's Office, MI; Orange County Sheriff's Department, CA; Phoenix Fire Department (2009-2010); Phoenix Police Department (2007-2008); Six Nations Tuscarora (2008-2010); and Seattle Fire Department (2009-2010).

TABLE OF CONTENTS

I GENERAL

II HOW TO

III REFERENCE

SECTION I

GENERAL

01

WHAT IS INTELLIGENCE?

WHAT IS INTELLIGENCE?

"National Intelligence and the term "intelligence related to national security" refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security."

United States Congress. "Intelligence Reform and Terrorism Prevention Act of 2004." Section 1012, Public Law 108-458--December 17, 2004

THE INTELLIGENCE COMMUNITY USES FIVE BASIC INTELLIGENCE SOURCES:

Geospatial Intelligence (GEOINT) is 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 composition of air and water samples.

Open-Source Intelligence (OSINT) is intelligence produced from publicly available information collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing 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 — includes 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. Gray Literature 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. The material cuts across scientific, political, socioeconomic, and military disciplines.
- Observation and Reporting — includes significant information not otherwise available that is/has been provided by amateur airplane spotters, radio monitors, and satellite observers among many others. The availability of worldwide satellite photography, often high resolution, on the Web (e.g., Google Earth) has expanded open-source capabilities into areas formerly available to major intelligence services only.

Signals Intelligence (SIGINT) is information 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, and/or analysis of the meaning of the communication.

- 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.

NOTES

07

WHAT INTELLIGENCE CAN AND CANNOT DO

WHAT INTELLIGENCE CAN AND CANNOT DO

"The United States Intelligence Community must constantly strive for and exhibit three characteristics essential to our effectiveness. The IC must be integrated: a team making the whole greater than the sum of its parts. We must also be agile: an enterprise with an adaptive, diverse, continually learning, and mission-driven intelligence workforce that embraces innovation and takes initiative. Moreover, the IC must exemplify America's values: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people."

~ National Intelligence Strategy 2009

Intelligence information can be an extremely powerful tool. It is most useful when the consumer has a clear understanding of what intelligence can and cannot do. While laws, policies, capabilities, and standards are constantly changing, these general guidelines can help consumers make the most of this resource.

1. **WHAT INTELLIGENCE CAN DO:** Intelligence can provide:

    - Decision advantage, by presenting information and analysis that can improve the decisionmaking process for consumers 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.

- Pre-travel security overviews and support.
- Reports on specific topics, either as part of ongoing reporting or upon request for short-term needs.
- Knowledge on persons of interest.

2. **WHAT INTELLIGENCE CANNOT DO:** Realistic expectations will help consumers fill their intelligence needs. Intelligence, however, cannot:

   - **Predict the future.** Intelligence can provide assessments of likely scenarios or developments, but there is no way to predict what will happen with absolute certainty.

   - **Violate U.S. law.** The activities of the Intelligence Community (IC) must be conducted consistent with all applicable laws and executive orders, to include the National Security Act of 1947, as amended; the Foreign Intelligence Surveillance Act; the Intelligence Reform and Terrorism Prevention Act (IRTPA); the Privacy Act of 1974; the Detainee Treatment Act; 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.


UNITED STATES INTELLIGENCE COMMUNITY
COLLABORATUS
VIRTUS
FIDES

11

THE INTELLIGENCE COMMUNITY

THE INTELLIGENCE COMMUNITY

"The United States intelligence effort shall provide the President, the National Security Council[1], and the Homeland Security Council[1], with the necessary information on which to base decisions concerning the development and conduct of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal."

- Executive Order 12333

The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC), overseeing and directing the implementation of the National Intelligence Program and acting as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. The U.S. IC is a coalition of 17 agencies and organizations within the Executive Branch that works both independently and collaboratively to gather the intelligence necessary for conducting foreign relations and protecting national security. The primary mission is to collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities require to execute their appointed duties. Some agencies focus on specific problem sets, use selected intelligence disciplines, or support a primary customer set, but their overall mission is the same – to protect the United States from all threats.

[1] As of May 2009, the Homeland Security Council and the National Security Council merged into the National Security Staff.

The activities of the IC include:

- Collection of information needed by the President, the National Security Staff, 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; and
- Such other intelligence activities as the President may direct from time to time.

The IC refers to those agencies and organizations as defined by the National Security Act of 1947, Sec 3, including such other elements of any department or agency as may be designated by the President or designated jointly by the Director of National Intelligence and the head of the department or agency concerned. Agencies, such as the Central Intelligence Agency, Defense Intelligence Agency, and National Security Agency perform intelligence as their primary function; others such as the Departments of State and Defense and military services perform intelligence in addition to other primary functions. The IC comprises the following 17 agencies and organizations:


Office of the Director of National Intelligence


Central Intelligence Agency


Defense Intelligence Agency


Department of Energy


Department of Homeland Security


Department of State


Department of the Treasury


Drug Enforcement Administration


Federal Bureau of Investigation


National Geospatial Intelligence Agency


National Reconnaissance Office


National Security Agency


U.S. Air Force Intelligence

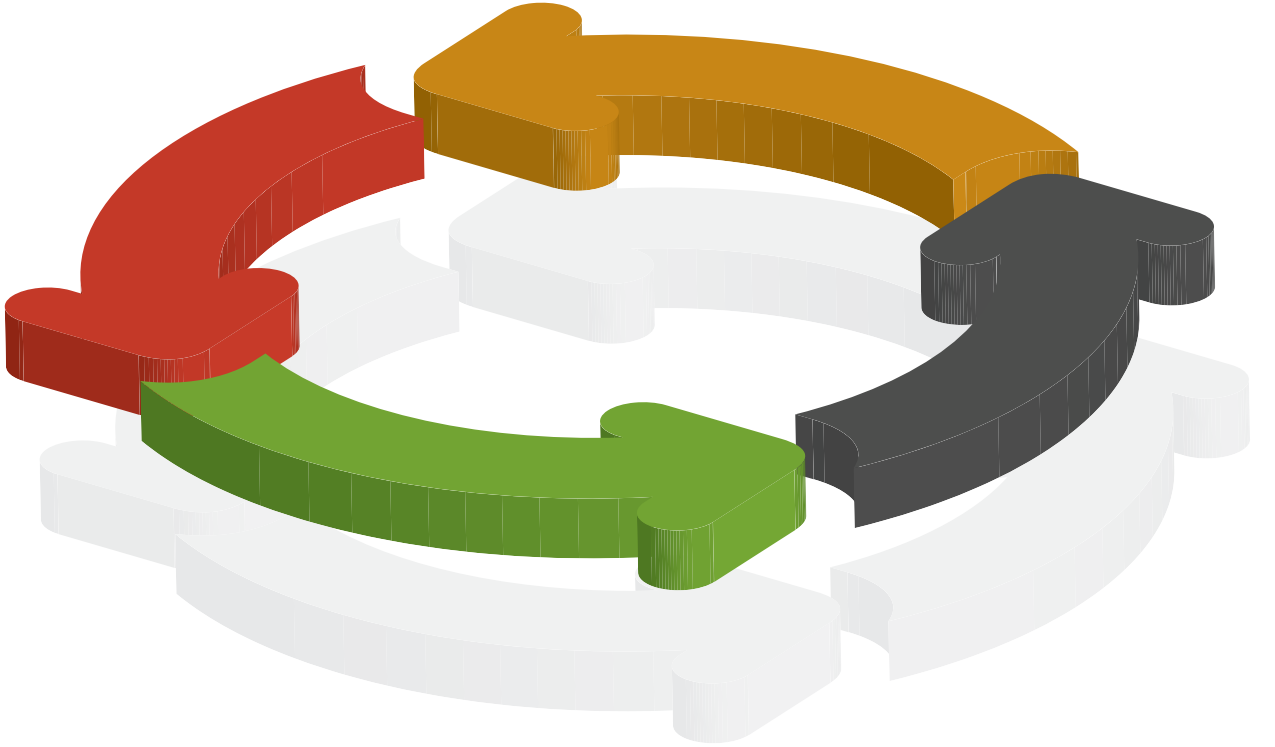

U.S. Army Intelligence


U.S. Coast Guard Intelligence


U.S. Marine Corps Intelligence


U.S. Navy Intelligence

NOTES



17

THE INTELLIGENCE CYCLE

THE INTELLIGENCE CYCLE

The intelligence cycle is the 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-ending and often includes a sixth stage of evaluation. Evaluation occurs for each of the stages individually and for the cycle as a whole. It is sometimes referred to as feedback.

SIX STEPS CONSTITUTE THE INTELLIGENCE CYCLE:

Planning and Direction: Establish the intelligence requirements of the consumer.

Planning and direction is the opening stage for the intelligence cycle. It is the springboard from which all intelligence activities are launched. Ironically, the direction portion will most often come first, whereby the consumer places a requirement for a specific product. The product may be a report, graphic, or at times raw intelligence. From that, the intelligence organization being tasked will plan its activity.

Collection: Gather the raw data required to produce the desired finished product.

Collection is accomplished by using any combination of the five basic intelligence sources or disciplines (Geospatial Intelligence, Human Intelligence, Measurement and Signature Intelligence, Open-Source Intelligence, and Signals Intelligence). The raw information gathered includes, but is not limited to, newspaper reporting, aerial imagery, satellite imagery, documents, and more.

Processing and Exploitation: Convert the raw data into comprehensible form that is usable for producing the finished product.

Processing and exploitation involves 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 processes and methods used for film, magnetic, and other media used for collecting and storing data.

Analysis and Production: Integrate, evaluate, analyze, and prepare the processed information for inclusion in the finished product.

Analysis and production requires highly trained, specialized personnel—analysts—to give meaning and priority to the information. Synthesizing the processed information into an actionable finished intelligence product allows the information to be 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 needs only the factual reporting or products such as raw imagery. This was the case during the Cuban Missile Crisis (October 1962) when 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: Deliver the finished product to the consumer who requested it and to others as applicable.

Dissemination is self-explanatory. Consumers who requested the information receive the finished product, usually via electronic transmission. This is accomplished most often using mechanisms such as Web sites, electronic mail, Web 2.0 collaboration tools, and hardcopy. The final and finished product is referred to as finished intelligence. After the product is disseminated, new intelligence gaps may be identified and the intelligence cycle begins again.

Evaluation: Acquire continual feedback during the cycle that aids in refining each individual stage and the cycle as a whole.

Evaluation is an assumed stage of the intelligence cycle and is not often discussed separately. One viewpoint maintains, however, that this stage must be understood and implemented along with the original five. Evaluation and feedback are important to allow the cycle and those using it to adjust and refine their activities and analysis to better meet consumers' information demands in the modern era.

NOTES


0
3

23

CATEGORIES OF FINISHED INTELLIGENCE

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 is disseminated directly to the customers whose initial needs generated the intelligence requirements. Finished intelligence is hand carried to the President and key national security advisers on a daily basis. The policymakers use the intelligence to make decisions. Their decisions may lead to requests for further examination, thus triggering the intelligence cycle one more time.

There are five categories of finished intelligence:

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 policymakers. It suggests urgency and implies the potential need to respond with policy action. Warning intelligence includes identifying or forecasting events that could cause the engagement of U.S. military forces or those that would have a sudden and detrimental effect on U.S. foreign policy concerns such as coups, third-party wars, or refugee situations. 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.

27

INTELLIGENCE PRODUCTS TYPICALLY AVAILABLE TO FIRST RESPONDERS

INTELLIGENCE PRODUCTS TYPICALLY AVAILABLE TO FIRST RESPONDERS

First responders can find intelligence products on a variety of classified and unclassified systems. Unclassified systems include Law Enforcement Online (LEO) and Homeland Secure Information Network (HSIN) on the Internet. First responders with the appropriate level of clearance and access can view classified information on National Counterterrorism Center (NCTC) CURRENT, the DHS Office of Intelligence and Analysis portal, and other sites on SECRET level systems, such as FBI Network (FBINet), Homeland Secure Data Network (HSDN), Joint Deployable Intelligence Support System (JDISS), and Secure Internet Protocol Router Network (SIPRNet). The types of products first responders will most likely encounter are:

Information Reports are messages that enable the timely dissemination of unevaluated intelligence within the Intelligence Community and law enforcement. These products include:

- FBI IIR (Intelligence Information Report)
- DHS HIR (Homeland Information Report)

Intelligence Assessments (IA) are finished intelligence products resulting from the intelligence analysis process. Assessments may address tactical, strategic, or technical intelligence requirements.

Intelligence Bulletins (IB) 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. IBs do not address threat warning information.

Threat Assessments (TA) or **Special Assessments (SA)** provide in-depth analyses related to a specific event or body of threat reporting and may address non-terrorist threats to national security.

Joint Products are intelligence assessments and bulletins produced jointly 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.

Other Products and Systems include intelligence summaries, briefs, and databases that cover counterterrorism, homeland security, and WMD-related information. Following are examples:

- **Joint Intelligence Bulletin (JIB).** The JIB provides timely information or analysis on a recent or current event or development of interest to all information and analysis customers and is produced at various classification levels. It focuses on Homeland Security issues, is written on an ad hoc basis, and is generally one to three pages. It is available on HSIN, LEO, or HSDN, depending on the classification of the information.

- **Roll Call Release (RCR).** Available on HSIN and LEO, the RCR is a collaborative For Official Use only (FOUO) product developed by DHS, FBI, and the ITACG. The product is written specifically for state, local, and tribal "street-level" first responders, and focuses on terrorist tactics, techniques, procedures; terrorism trends; and potential indicators of suspicious activity. The product is written on an ad hoc basis, is focused on one subject, and fits on one page.

- **Terrorism Summary (TERRSUM).** The TERRSUM is a SECRET digest of terrorism-related intelligence of interest to Federal and non-Federal law enforcement, security and military personnel. Produced Monday through Friday, the TERRSUM includes terrorism-related intelligence available to NCTC and other Intelligence Community elements. The product is available on SECRET-level systems to appropriately cleared personnel at state and major urban area fusion centers and Joint Terorrism Task Forces.

- **Worldwide Incidents Tracking System (WITS).** WITS is the U.S. Government's authoritative database on terrorist attacks compiled exclusively from open-source information. Maintained by the NCTC, WITS is publicly available at www.nctc.gov. Users can search for attack data and sort it by a broad range of characteristics, to include type of attack, location, facility, perpetrator, and other attributes. Users also can plot incidents on maps using Google Earth and Google Map. State, local, and tribal law enforcement and first responders use WITS to track terrorist trends, support event planning, and provide context for terrorist activities.

NOTES

33

JOINT PARTNERSHIPS

JOINT PARTNERSHIPS

"Our enemies live in the seams of our jurisdictions. No single agency or nation can find them and fight them alone. If we are to protect our citizens, working together is not just the best option, it is the only option."

- FBI Director Mueller, Global Terrorism Today and the Challenges of Tomorrow

Federal, state, local, and tribal governments understand the benefits and value of working together and have established several programs to protect the United States within our borders. These programs include Joint Terrorism Task Forces, the National Joint Terrorism Task Force, the State and Major Urban Area Fusion Centers and the National Operations Center. These programs leverage the broad experience, knowledge, and skills of personnel from a wide variety of fields, such as intelligence, law enforcement, fire, and emergency services.

Joint Terrorism Task Force (JTTF). JTTFs serve as the coordinated "action arms" for federal, state, and local government response to terrorist threats in specific U.S. geographic regions. The FBI is the lead agency that oversees JTTFs. The benefits of a JTTF include:

- "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; and
- familiarity among agencies, investigators, and managers before a crisis occurs.

The mission of a JTTF is to leverage the collective resources of the member agencies for the prevention, preemption, deterrence, and investigation of terrorist acts that affect United States interests, to disrupt and prevent terrorist acts, and to apprehend individuals who may commit or plan to commit such acts. To further this mission, a JTTF serves as a means to facilitate information sharing among JTTF members.

- As of January 2011, there are 104 JTTFs based nationwide, including at least one in each of the FBI's 56 field offices.

- More than 600 state and local agencies participate in JTTFs nationwide. Federal representation includes the U.S. Intelligence Community, the Departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and Interior, among others.

Fusion Centers. A fusion center is a dedicated element, run by the applicable state or local jurisdiction, that 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 fusion center is defined as 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 intelligence and fusion 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 state and local law enforcement 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 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.

- As of January 2011, there are 72 designated fusion centers (50 state and 22 Major Urban Areas).

- Fusion centers are designed to involve every level and discipline of government, private-sector entities, and the public—though the level of involvement of some participants will vary.

- Fusion centers are state and locally owned and operated. The Department of Homeland Security (DHS) has a statutory program to support fusion centers.

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. Analytic and information-sharing efforts carried out by the JTTFs are done solely to support those investigative efforts. Also each FBI office contains a Field Intelligence Group which is the main interlocutor with the fusion center. **Fusion centers**, in contrast, are information sharing and analytic entities and do not focus solely on terrorism. They are state and locally owned and operated information analysis centers that analyze information and intelligence regarding a broad array of criminal and other activities related to homeland security. Fusion centers focus on trend and pattern analysis that is intended to help state and local law enforcement mitigate emerging crime problems, including terrorism and other threats to homeland security.

National Joint Terrorism Task Force (NJTTF). The mission of the NJTTF is to enhance communication, coordination, and cooperation between 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 the JTTFs throughout the United States.

- The NJTTF was established in July 2002 to serve as a coordinating mechanism with the FBI's partners.

- As of January 2011, forty-nine agencies are represented in the NJTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple partners.

National Operations Center (NOC). The mission of the NOC is to serve as the primary National-level hub for domestic situational awareness, common operating picture, information fusion, information sharing, communications, and operations coordination pertaining to the prevention of terrorists attacks and domestic incident management.

The NOC serves as the nation's nerve center for information collection and sharing. Pursuant to section 515 of the Homeland Security Act of 2002 the NOC is the principal operations center for DHS. As the principal operations center, Congress tasked the NOC with performing two key responsibilities:

- First, the NOC shall provide situational awareness and a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other man-made disaster.

- Second, the NOC shall ensure that critical terrorism and disaster-related information reaches government decision-makers. By performing its mission, the NOC enables the Secretary DHS and other leaders to make informed decisions and identify courses of action during an event or threat. The Secretary has assigned the NOC to the DHS Office of Operations Coordination and Planning (OPS).

The NOC is comprised of five operational components: the NOC-Watch, Federal Emergency Management Agency National Response Coordination Center (NRCC), DHS National Infrastructure Coordinating Center (NICC), Office of Intelligence and Analysis/Intelligence Watch and Warning Branch and the OPS Planning Element. Each NOC operational component remains an independent entity under the program management of its parent DHS Component. By drawing upon and leveraging the authorities and capabilities of each NOC operational component, the NOC—as a cohesive and integrated whole—serves as the primary national hub for situational awareness and operations coordination across the federal government for incident management and as the national fusion center, collecting and synthesizing all-source information, including information from the state fusion centers, across all-threats and all-hazards information covering the spectrum of homeland security partners.

SECTION II

How To


FRAGILE
HANDLE WITH CARE
FRAGILE
HANDLE WITH CARE

41

HANDLING UNCLASSIFIED INFORMATION

HANDLING UNCLASSIFIED INFORMATION

Federal agencies routinely generate, use, store, and share information that, although does not meet the standards for Classified National Security Information under Executive Order 13526 of December 29, 2009, is sufficiently sensitive to warrant some level of protection, in accordance with Executive Order 13556, Controlled Unclassified Information (CUI), signed November 4, 2010. First responders should be aware of the federal handling requirements for sensitive or CUI to ensure it is used only by those who need it and only for its intended purpose.

Until official implementing instructions and markings are provided by the Information Security Oversight Office (ISOO) to denote CUI, government agencies shall continue to use dissemination control markings such as FOR OFFICIAL USE ONLY (FOUO), LAW ENFORCEMENT SENSITIVE, SENSITIVE BUT UNCLASSIFIED, and OFFICIAL USE ONLY. In many instances the requirements for safeguarding this information are equivalent; however, these current markings may change substantially once CUI markings have been developed, approved and adopted for implementation throughout the Federal Government.

FOUO, per 32 CFR Section 286.15 and CUI, per Executive Order 13556, is information that has not been given a security classification pursuant to Executive Order 13526-National Security Information, but which may be witheld from the public because disclosure would cause a forseeable harm to an interest protected by one or more Freedom Of Information Act (FOIA) exemptions. FOUO and CUI shall be considered as warranting protection or safeguarding.

FOUO is not a classification, but one of the most widely used dissemination control markings. It is used typically though not consistently throughout government to identify unclassified information of a sensitive nature that may or may not otherwise be categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or other government interests.

Dissemination of FOUO is typically restricted to persons with "need-to-know". Need-to-know 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 typical FOUO requirements include:

- 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 must have valid need-to-know, and precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

Information labeled FOUO or any other control marking needs to be safeguarded and withheld from public release until such time as the originating agency clarifies the nature of the handling requirements and/or approves it for public release.

45

PROCESSING SECURITY CLEARANCES

SECURITY CLEARANCES

Most information needed by state, local, and tribal first responders can be shared at an UNCLASSIFIED level. In instances where it is necessary to share classified information, it can usually be accomplished at the SECRET level.

State and local officials who require access to classified material must apply for a security clearance through FBI or DHS. The clearance process involves completing a questionnaire for National Security Positions, submitting fingerprints, and undergoing a background investigation. Record checks for SECRET and TOP SECRET security clearances are required for a security clearance to be granted, and cannot be waived.

SECRET Clearance. A SECRET security clearance may be granted to those persons who need access to or who need to know national security information classified at the CONFIDENTIAL or SECRET level. A SECRET security clearance takes the least amount of time to process.

- Records checks with various Federal agencies and local law enforcement as well as a review of credit history are conducted.

- Candidate completes the SF-86 Questionnaire for National Security Positions and the FD-258 Applicant Fingerprint Card. Once favorably adjudicated for a SECRET security clearance, the candidate will be required to sign a nondisclosure agreement.

TOP SECRET Clearance. A TOP SECRET security clearance may be granted to those persons who need to know national security information classified up to the TOP SECRET level and who, when necessary, need unescorted access to sensitive facilities.

- In addition to satisfying all requirements for a clearance at the SECRET level, a background investigation covering a 10-year time period is required.

- Once favorably adjudicated for a TOP SECRET security clearance, the candidate will be required to sign a nondisclosure agreement.

Questions and Answers

Q: Who should apply for a security clearance?

A: Officials whose duties require that they have access to classified information and who are willing to undergo a mandatory background investigation.

Q: What is the purpose of a background investigation?

A: A background investigation is conducted to allow the government to assess whether a candidate is sufficiently trustworthy to be granted access to classified information. Applicants must meet certain criteria relating to their honesty, character, integrity, reliability, judgment, mental health, and association with undesirable persons or foreign nationals. The scope of the investigation varies with the level of the clearance being sought.

Q: What kind of inquiries will be made into my background?

A: Credit and criminal history checks will be conducted on all applicants. For a TOP SECRET security clearance, the background investigation includes additional records checks which can verify citizenship for the applicant and family members, birth, education, employment history, and military history.

In addition, interviews will be conducted with persons who have known the candidate and with any spouse divorced within the past 10 years. Additional interviews will be conducted, as needed, to resolve any inconsistencies. Residences will be confirmed, neighbors interviewed, and public records queried for information about bankruptcies, divorces, and criminal or civil litigation.

The background investigation may be expanded if an applicant has resided abroad, or has a history of mental disorders, or drug or alcohol abuse.

A personal interview will be conducted of the candidate.

Q: Are there advantages or disadvantages to receiving unclassified or classified terrorism-related information?

A: An advantage of receiving unclassified terrorism-related information is that there may be fewer restrictions on an official's ability to further disseminate it within the official's jurisdiction. Classified information may be disseminated only to other cleared persons who also have a need-to-know.

For additional information, please contact your local FBI field office or state or major urban area fusion center.

NOTES

51

ACCESSING INTELLIGENCE COMMUNITY INFORMATION

ACCESSING INTELLIGENCE COMMUNITY INFORMATION

Classified and unclassified information can be accessed by first responders through multiple systems and Web sites. In some cases an account is required, although in others all that is needed is access to a specific computer network. Some sources of information require only that an individual perform homeland security or law enforcement activities on behalf of a state, local, or tribal government; a few require specific security clearances and access to secure systems.

UNCLASSIFIED INTELLIGENCE PRODUCTS

Homeland Security Information Network (HSIN). HSIN is a comprehensive, nationally secure and trusted Web-based platform able to facilitate information sharing and collaboration between federal, state, local, tribal, private-sector, and international partners.

- HSIN has five major mission areas or Communities of Interest (COI) that allow federal, state, and local organizations, private-sector partners, critical-sector organizations such as utility companies, fusion centers, and government agencies with multiple missions to collaborate. The five mission areas are Intelligence and Analysis, Law Enforcement, Emergency Management, Critical Sectors, and Multi-Mission Agencies.

- Access: A request for nomination must be sent by a COI owner or an authorized nominator, or requestor must send a request for membership via e-mail to HSIN at helpdesk@dhs.gov or call 1-866-430-0162. Please include the COI (Intelligence and Analysis, Law Enforcement, Emergency Management, Critical Sectors, or Multi-Mission Agencies) to which the requestor desires membership, along with their name, official e-mail address, organization, supervisor's name, and a phone number. Requests received via e-mail will be forwarded to the appropriate COI owner for consideration.

Homeland Security Information Network-Intelligence (HSIN-Intel). HSIN-Intel is a Web portal that hosts two COIs of particular interest to intelligence analysts engaged in the homeland security arena: the Federal, State, Local, and Tribal (FSLT) COI and the Homeland Security State and Local Intelligence COI (HS SLIC). The difference between the two COIs is that HS SLIC contains Sensitive Personally Identifiable Information (SPII) and requires two-factor authentication for access: a password and an electronic security token.

- Access: The HS SLIC is a charter-based organization requiring both individual and organizational membership. Contact the HS SLIC helpdesk at hs.slic@hq.dhs.gov for more information. HS SLIC eligibility requirements include:
    - Engagement in intelligence analysis functions.
    - Employment by a law enforcement, criminal justice, or homeland security agency.
    - Engagement in detecting, defeating, or deterring terrorist acts.
    - U.S. citizenship.
    - A government e-mail address (federal, state, or local).
    - Association with a fusion center (for state and local participants and federal officers in the field).

Those who do not meet the requirements of the HS SLIC may request access to the FSLT community by contacting ia.pm@dhs.gov.

Intelink-U. Intelink-U is the Intelligence Community's (IC) sensitive but unclassified-sharing network. Content is provided by the IC, other government agencies, foreign partners, academia, and open sources. Accounts are available to individuals with federal, state, local, and tribal homeland security and law enforcement responsibilities.

- Web site: https://www.intelink.gov.
- Access: Go to Web site, click on "Sign In," and proceed to "New Account Registration."

Law Enforcement Online (LEO). LEO can be accessed from any computer system with an Internet connection. It is an official government information-sharing and electronic-communications portal. LEO provides FBI, joint FBI-DHS, NCTC, and non-federally produced intelligence products at the For Official Use Only (FOUO) level. Accounts are available to federal, state, local, and tribal personnel performing homeland security or law enforcement duties and personnel from foreign law enforcement agencies.

- Web site: http://www.leo.gov.
- Access: Go to Web site, click on the "LEO Membership Criteria," then the "LEO User Application," or contact the LEO helpdesk at 1-888-334-4536, or via e-mail at helpdesk@leo.gov.

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. Featured are 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 some of the most renowned thinkers

on national security issues inside and outside the U.S. Government. Accounts are available to federal, state, and local government employees and contractors.

- Web site: http://www.opensource.gov.
- Access: Apply online via Web site.

Regional Information Sharing Systems Network (RISSNET). RISSNET facilitates information sharing within the law enforcement community to combat multijurisdictional criminal activities and conspiracies. It is composed of six multistate intelligence centers (RISS Intelligence Centers). Membership includes federal, state, local, and tribal law enforcement agencies. Access is requested through the regional RISS Intelligence Centers.

- Web site: http://www.riss.net.
- Contact information available at http://www.riss.net/Centers.aspx.

Technical Resources for Incident Prevention (TRIPwire). TRIPwire is the Department of Homeland Security's 24/7 online, secure, collaborative, information-sharing network for bomb squad, law enforcement, and other emergency services personnel to learn about current terrorist Improvised Explosive Device (IED) tactics, techniques, and procedures, including design and emplacement considerations. TRIPwire combines expert analysis and reports with relevant documents, images, and videos gathered directly from terrorist sources to help law enforcement anticipate, identify, and prevent IED incidents.

- Web site: https://www.tripwire.dhs.gov.
- Access: For more information about the TRIPwire system, please contact the Office for Bombing Prevention at OBP@dhs.gov or through the TRIPwire help desk at help@tripwire-dhs.net.

SECRET INTELLIGENCE

Access to the following classified systems requires, at a minimum, a SECRET security clearance.

NCTC CURRENT (formerly NCTC Online). NCTC CURRENT, the IC's terrorism resource, can be accessed from any SECRET U.S. Government information system (HSDN, FBINet, JDISS, or SIPRNet).

- Web site: https://current.nctc.sgov.gov.
- Access: Authorized access to HSDN, FBINet, JDISS, or SIPRNet and a valid Intelink Passport.

Office of Intelligence and Analysis (I&A) Web page, DHS. The I&A homepage can be accessed from any SECRET U.S. Government information system (HSDN, FBINet, JDISS, or SIPRNet).

- Web site: http://dhs.csp.sgov.gov.
- Access: Authorized access to HSDN, FBINet, JDISS, or SIPRNet.

FBINet. The FBI intranet can be accessed only from an FBINet computer.

- Web site: http://intranet.fbinet.fbi.
- Access: Authorized access to an FBINet system.

FBI Intelink/SIPRNet. The Web site can be accessed from any SECRET U.S. Government information system (HSDN, FBINet, JDISS, or SIPRNet).

- Web site: http://www.fbi.sgov.gov.
- Access: Authorized access to HSDN, FBINet, JDISS, or SIPRNet.

Open Source Center (OSC). The OSC and its partners provide timely and tailored translations, reporting, and analysis on foreign policy and national security issues.

- Web site: http://www.opensource.sgov.gov.
- Access: Authorized access to HSDN, FBINet, JDISS, or SIPRNet and an OSC account.

NOTES


THIS CARTON HAS BEEN SEAL
SECURITY TAPE
WARNING-WARNIN
IF THIS SEAL IS BROKEN CHECK
CONTENTS BEFORE ACCEPTANCE

59

UNDERSTANDING THREAT INFORMATION

UNDERSTANDING THREAT INFORMATION

First responders are likely to receive threat information during breaking events of national interest. The threat information can be in the form of a raw intelligence report, alert, warning, or notification and provides timely dissemination of unevaluated intelligence within the U.S. intelligence, federal law enforcement, and state, local, tribal and private sector communities. This is information that individuals or organizations need in order to make decisions. To get the most benefit from these products, it is important to have a general understanding of the criteria that the intelligence community typically uses to create them.

The Intelligence Community uses the following criteria to understand threat information:

Access. Addresses the ability of the source to obtain the information. Some commonly used levels of source access are:

- Excellent – Excellent refers to firsthand observation. All technical sources have excellent access.

- Good – A source has good access if the source learns information from a subsource directly involved in a private conversation. A source may have good access if the source directly overhears a conversation, without knowledge of the conversation's participants.

- Direct – The intelligence source has direct knowledge of the intelligence fact reported or appears to be in the direct contact with those involved or knowledgeable.

- Indirect – Indirect access refers to any source access that is determined not to be excellent or good.

Credibility. The term refers to the extent to which something is believable. This term is commonly used with reference to sources of evidence, to evidence itself, and to hypotheses based on evidence. The term reliability is sometimes used as a synonym for credibility, but this causes difficulties. Reliability is only one attribute of the credibility of certain forms of evidence. The credibility of sources of evidence is both context and time dependent. A person or a source may be more credible regarding certain events and at certain times but not so credible regarding other events or at other times. Typically, information may be assessed as being credible or noncredible, or as levels of credibility (low credibility or high credibility).

Reliability. A subcriteria of credibility applied to the primary source provides a likelihood that the most recent reporting can be assessed to be an accurate representation of the events reported on the basis of the past performance of the source. This subcriteria is an analyst's judgment of the intelligence source for a particular report. The following terms and amplifications are used in describing source reliability:

- SOURCE: (U) An established source with indirect access, much of whose reporting has been corroborated over the past eight years.

- SOURCE: (U) A collaborative source with excellent access, some of whose reporting has been corroborated over the past two years.

Context Statement: A context statement is optional and describes, in greater detail than the source byline, the circumstances under which the source acquired the intelligence contained in the report. To the extent possible, it should also address the source's reporting history or other pertinent information regarding source credibility in a discrete statement. For example, if a trusted source begins reporting on information substantively different than the sort of information the source previously had access to, a report author might use the following statements:

- CONTEXT: (U) Source claimed firsthand access to the information provided in this report.
- CONTEXT: (U) This information was obtained through a lengthy chain of acquisition, and the ultimate subsource cannot be determined.

Chain of Acquisition. This element addresses source relationships and potential changes in the information as it passed from one person to another. The longer the chain of acquisition (the more people who obtained and relayed the information) the more likely the information changed, a factor affecting the accuracy of the information.

Source Categories. The Intelligence Community distinguishes the source of the information to assist in understanding threat information. The following terms and distinctions are commonly used in describing sources:

- **One-time Contact:** This category is for one-time contacts who are providing information voluntarily and in confidence, but with whom there is no previous contact. Inclusion of a context statement is strongly recommended for all first-time or one-time source entries. For example:

    - SOURCE: (U) A contact with [direct/indirect/good/excellent] access who spoke in confidence. This is the first reporting from the source, reliability cannot be determined.

    - CONTEXT: (U) We have no further information to corroborate the following report. The source of the following information is a contact whose access is unknown and whose motivations for providing the information are unclear.

- **Limited Contact:** This category is for contacts who have provided information more than once, but who still do not have an established reporting record. As with a one time contact, inclusion of a context statement is strongly recommended. For example:

    - SOURCE: (U) A contact with [direct/indirect/good/excellent] access whose reporting history is limited and whose reliability cannot be determined.

- **Contact Who Spoke in Confidence:** For private sector sources who voluntarily alert federal law enforcement to various suspicious activities. These sources provide reliable information that is gained in the course of their ordinary duties.

    - SOURCE: (U) A contact with [direct/indirect/good/excellent] access who spoke in confidence and whose reporting, though limited, has been reliable in the past.

- **Collaborative Source:** This category is for individuals with whom there is a formal relationship. The reliability statement is based on a combination of the quality and quantity of the source's reporting. For example:

    - SOURCE: (U) A collaborative source with [direct/indirect/good/excellent] access, [some/much/all] of whose reporting has been corroborated over the past [number] years.

- **Established Source:** This category is primarily for sources with whom there is a long term relationship and who are responsive to tasking.

    - SOURCE: (U) An established source with [direct/indirect/good/excellent] access, [some/much/all] of whose reporting has been corroborated over the past [number] years.

- **Walk-in/Write-in/Call-in:** This category is for individuals who volunteer information on their own, with or without requesting some sort of assistance in return. Inclusion of a context statement should be considered for sources that fit this category.

    - SOURCE: (U) A walk-in to this agency.
    - SOURCE: (U) A write-in to this agency.
    - SOURCE: (U) A write-in to an official U.S. Government web site.

    - SOURCE: (U) A call-in to this agency.

    - CONTEXT: (U) We have no further information to corroborate the following report. The source of the following information is a walk-in who claimed firsthand access to the information provided in the report. The source's motivations for providing the information are unclear.

- **Detainee:** This category is used for interviews of detainees in custody, and that are held as enemy combatants (i.e., outside of the usual civilian and military U.S. criminal justice systems).

    - SOURCE: (U) A detainee.

- **Foreign Government Information:** This category is used for information received as part of an official exchange from a foreign intelligence, security, or police service with which there is a formal relationship.

    - SOURCE: (U) Foreign government information.

- **FBI Special Agent (SA):** This category is used for reporting firsthand observations made by FBI SAs. A report should only be sourced to an FBI SA if the FBI agent's personal investigative initiative, actions, and investigative methods used led to the information's acquisition by the FBI.

    - SOURCE: (U) An FBI agent.

- **Employee of the FBI:** This category is used for reporting firsthand observations made by FBI employees that are not SAs.

    - SOURCE: (U) An employee of the FBI.

- **Officer of Another Law Enforcement Agency:** This category is used for reporting information provided by another U.S. law enforcement agency (that is, federal, state, local, or tribal).
    - SOURCE: (U) Officer of another law enforcement agency.
- **Officer of Another U.S. Government Entity (non-law enforcement):** This category is used for reporting information provided by another U.S. Government Entity that is not a law enforcement agency, task force, or other entity (federal, state, local, or tribal).
    - SOURCE: (U) Officer of another U.S. Government Entity.
- **Sensitive Source:** This category is used for information obtained using sensitive technical investigative methods. If a report contains information from more than one technical source, they may all be folded into one byline.
    - SOURCE: (U) Sensitive source with excellent access.
- **Documentary Source:** This category is used for all types of media with recorded/printed information, regardless of the nature of the media or method(s) of recording.
    - SOURCE: (U) Documentary source.
- **A Bank Secrecy Act (BSA)-Derived Information Report:** This category is used for any information derived from reporting authorized under the BSA, as administered by the Financial Crimes Enforcement Network (FinCEN). This byline should always be used in conjunction with a context statement that identifies the exact type of BSA report from which the information is derived.
    - SOURCE: (U) A Bank Secrecy Act-derived information report.
    - CONTEXT: (U) A suspicious activity report.

- **Multiple Sources:** When a report has multiple sources, it is very important to preserve and separate which source provided which information. Any sources, contacts, walk-ins/call-ins/write-ins, government employees, or detainees that contribute to a report must feature their own source byline.

Additional Source Statement Examples:

- "Source obtained the information from a reliable subsource with direct access."
- "Source obtained the information from a subsource whose reporting record has not been established."
- "Source was aware that his information would reach the U.S. Government and may have intended his remarks to influence as well as to inform."
- "The veracity of this source's information is seriously doubted but is being reported here because of the nature of the threat discussed."
- "The information was provided by the source who spoke in confidence and without the knowledge of his government's superiors. The information may not be discussed with any foreign government officials, especially those of the source's government."
- "The information provided in this report may have been intended to influence as well as to inform."

69

UNDERSTANDING ESTIMATIVE LANGUAGE

UNDERSTANDING ESTIMATIVE LANGUAGE

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

Intelligence judgments pertaining to likelihood are intended to 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 words 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 is unable to 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 its judgments.

- **High confidence** generally indicates that the IC's judgments are based on high-quality information and/or that the nature of the issue makes it possible to render a solid judgment.

- **Moderate confidence** generally means that the information is interpreted in various ways, that the IC has alternative views, or that the information is credible and plausible but not corroborated sufficiently to warrant a higher level of confidence.

- **Low confidence** generally means that the information is scant, questionable or very fragmented, and it is difficult to make solid analytic inferences, or that the IC has significant concerns or problems with the sources.


FOCUS/
AE LOCK
EVF/LCD
DISPLAY
OFF
ON

73

REPORTING SUSPICIOUS ACTIVITY

REPORTING SUSPICIOUS ACTIVITY

"Whether a plan for a terrorist attack is homegrown or originates overseas, important knowledge that may forewarn of a future attack may be derived from information gathered by state, local, and tribal government personnel in the course of routine law enforcement and other activities."

- National Strategy for Information Sharing, October 2007

Because of the nature of their work, the more than 800,000 law enforcement and 1.2 million firefighters in the United States are perfectly poised to identify criminal activity that may be percursor indicators of acts of terrorism. In many instances information that is 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, and private-sector partners.

Suspicious activity reporting should be made available to your local area fusion centers and Joint Terrorism Task Forces (JTTF) in a timely manner.

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

The NSI is a comprehensive and coordinated effort to establish a "unified process for reporting, tracking, and accessing SARs" in a manner that rigorously protects the privacy and civil liberties of Americans. The NSI strategy is to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities. The long term goal is that federal, state, local, and tribal law enforcement organizations, as well as the private sector, will participate in a standardized and integrated approach to SAR.

What is a SAR and why is it important?

Law enforcement entities carry out counterterrorism-related activities as part of their duty to protect local communities from crime and violence. It is important that first responders who recognize criminal behaviors and incidents associated with the planning and carrying out of a terrorist attack document and share this information via a SAR.

The SAR Process

All agencies, regardless of size or jurisdiction, have a role in the nationwide SAR process. It is essential that state, local, tribal, and federal agencies establish standardized SAR programs and work together to share SAR information in order to prevent and deter terrorist attacks on American soil. There are five basic cornerstones to implementing the SAR process:

- **Stakeholder management** - Knowing, understanding, and communicating with all stakeholders is key to success. The chief executive and agency leadership must recognize the importance of implementing a SAR process within their agency and champion the efforts of the SAR process and the NSI both inside and outside the agency. Outreach to the community is being done through an initiative called, Building Communities of Trust and is also being done in collaboration with the "If you see something, say something" campaign launched by the Department of Homeland Security in July 2010.

- **Training** – The NSI training strategy is a multifaceted approach designed to increase the effectiveness of state, local, and tribal law enforcement professionals in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. The overarching goal of the training strategy is to facilitate agency implementation of the SAR process, ensure the inclusion of civil rights, civil liberties and privacy safeguards, and to enhance a nationwide SAR capability. There

are currently three trainings: Chief Executive Briefing, Analyst Training, and Line Officer Training. In an attempt to reach all 800,000 law enforcement officers, the Line Officer Training is available in several online platforms, including www.mipt.org and www.leaps.tv.

- **Privacy and Civil Liberties Protections** - The NSI requires each site to consider privacy throughout the SAR process by fully adopting the following NSI Privacy Protection Framework prior to NSI participation. This framework includes a privacy policy that is at least as comprehensive as the ISE Privacy Guidelines, compliance with the most current ISE-SAR Functional Standard, and completion of the privacy trainings.

- **Enabling Technology** - To support the operational mission, NSI Federated Search facilitates information sharing using the National Information Exchange Model (NIEM), allowing searches across a federated environment that uses a standardized data format. The FBI's eGuardian system has been fully integrated into the NSI Federated Search.

It is critical that SAR information be submitted to the NSI Federated Search, including e-Guardian so it can be shared with the nation's JTTFs.

- **Operational Process** - The most important component of the program is supporting the operational mission. The job of homeland security, safety, or justice cannot be relegated to a fragmented approach, making a standards-based method for the gathering, processing, reporting, analyzing, and sharing of suspicious activity (also referred to as the SAR process) necessary. It is critical that there be integration of state, local, and tribal law enforcement agencies' SAR processes into this nationwide effort.

SAR Initiative Resources

The following links are valid as of January 2011 and may be available on other government websites

- Guidance for Building Communities of Trust
  http://nsi.ncirc.gov/documents/e071021293_BuildingCommTrust_v2-August%2016.pdf

- Privacy, Civil Rights, and Civil Liberties Protections: A Key Component of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) http://nsi.ncirc.gov/documents/NSI_Privacy_Briefing.pdf

- NSI Training Overview http://nsi.ncirc.gov/documents/NSI_Training_Overview.pdf

- National Strategy for Information Sharing: http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html

- Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project: www.it.ojp.gov/documents/SARReportOctober2008.pdf

- Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR): http://nsi.ncirc.gov/resources.aspx

- National Information Exchange Model: www.niem.gov

- Additional resources and publications on the SAR initiative or the SAR process can be located at:

    - nsi.ncirc.gov
    - www.ise.gov

NOTES

SECTION III

REFERENCE

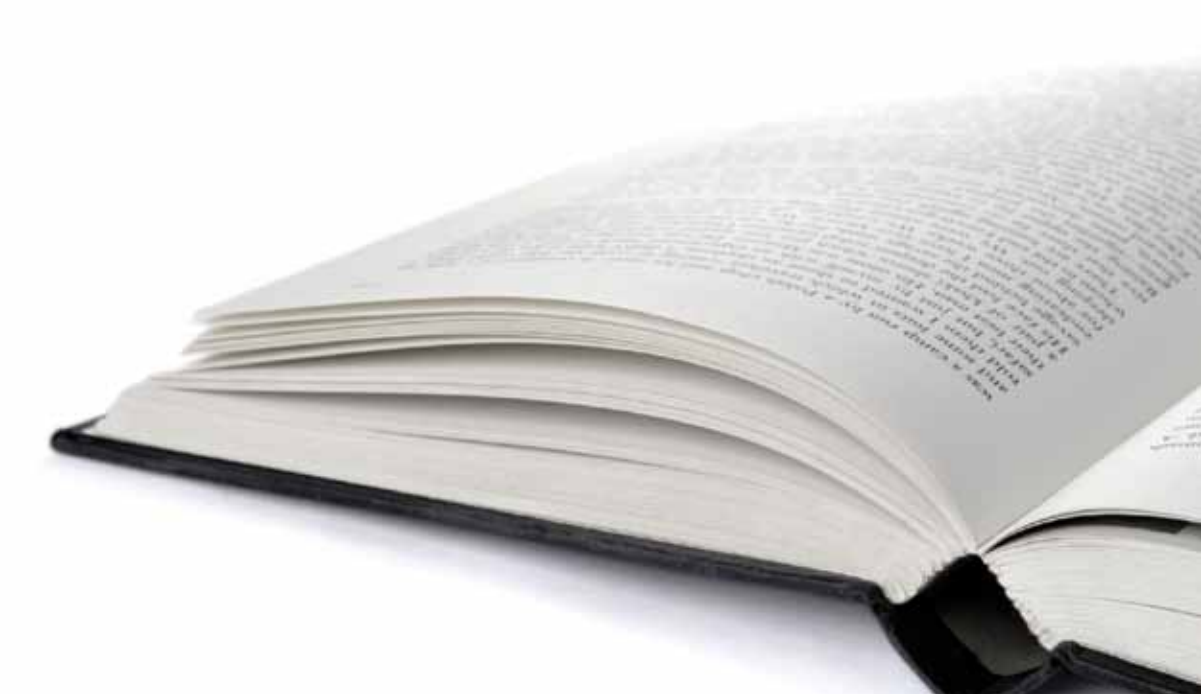

LIBRARY

81

INTELLIGENCE COMMUNITY TERMINOLOGY

INTELLIGENCE COMMUNITY TERMINOLOGY

Terminology used in intelligence circles may seem straightforward at first glance, but the definitions often differ from conventional use. The following list of terminology is not exhaustive and contains the terms which are likely to be encountered by first responders reading intelligence material. While there may be other definitions for these terms, the definitions used in this guide were selected to be the most relevant to the first responder audience.



A

Access: The means, ability, or permission to approach, enter, or use a resource.

Actionable: (1) Information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process; it 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.

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 several or all of the intelligence disciplines including SIGINT, HUMINT, MASINT, OSINT, and GEOINT.

Analysis: The process by which people transform information into intelligence; systematic examination in order 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 in evaluating subsequent information.

Behaviors: Observable actions one uses to achieve results.

C

Case Officer: A professional employee of an intelligence organization who is responsible for providing direction for an agent operation.

Clandestine Activity: An activity that is usually extensive, goal-oriented, planned, and executed to conceal the existence of the operation. Only participants and the agency sponsoring the activity are intended to know about the operation. "Storefront" operations, "stings," and certain concentrated undercover investigations can be classified as clandestine activities.

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 at issue and placement of useful information into a form or system that permits easy and rapid access and retrieval.

Collateral Information: National security information classified TOP SECRET, SECRET or CONFIDENTIAL that is not sensitive compartmented information.

Collection (of information): The identification, location, and recording/storing of information—typically from an original source and using both human and technological means—for input into the intelligence cycle for the purpose of meeting 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 the purposes of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, and/or analysis of the substantive meaning of the communication. COMINT is a sub-discipline of SIGINT.

Conclusion: A definitive statement about a suspect, action, or state of nature based on the 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 gain the views of other producers on the adequacy of a specific draft assessment, estimate, or report; it is intended to increase a product's factual 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 and/or acts, both real and imputed. (2) A strategy intended to prevent or counter terrorism.

Covert: Planned and executed to conceal the collection of information and/or the identity of any officer or agent participating in the activity. Intelligence operations conducted in secrecy.

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 United States, 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 thereto, 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/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 the interception of the communications by an unauthorized or unintended party.

Current Intelligence: Intelligence of all types and forms of immediate interest to the users of intelligence; 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 which provides notification to each agency involved of the shared interest in the case, as well as providing contact information. This is 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 taking information and arriving at conclusions from within that information.

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 intelligence 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, analytical procedures, or privileged information in order to permit wider distribution.
(See Sanitization.)

E

Electronics 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 of this type of information are radar signals. ELINT is a sub-discipline of SIGINT.

Essential Elements of Information: Items of intelligence information essential for timely decisions and for enhancement of operations that relate to foreign powers, forces, targets, or physical environments. (See Priority Intelligence Requirement.)

Estimate: (1) An 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. (2) An appraisal of the capabilities, vulnerabilities, and potential courses of action of a foreign nation or combination of nations in consequence of a specific national plan, policy, decision, or contemplated course of action. (3) An 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 project 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 that is responsible for the management, execution, and coordination of intelligence functions within the field office region.

Finished Intelligence: The intelligence product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information.

Foreign Disclosure Officer (FDO): A person specifically designated in writing who is authorized to release and/or disclose classified and controlled unclassified information to foreign governments and international organizations. Intelligence Community directives require all classified and controlled unclassified information to be specifically authorized by an FDO prior to release.

Foreign Instrumentations 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. FISINT is a sub-discipline of SIGINT.

Foreign Intelligence Surveillance Act (FISA): The FISA of 1978, as amended, prescribes procedures for the collection of 'foriegn intelligence information' by electronic surveillance, physical search, and other means. FISA is codified at 50 U.S.C. 1801 et seq.

For Official Use Only (FOUO): (1) Per 32 CFR Section 286.15, information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be witheld from the public because disclosure would cause a forseeable harm to an interest protected by one or more Freedom Of Information Act (FOIA) exemptions shall be considered as being FOUO.

(2) 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 impact 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 access 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 to the center 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: 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 TOP SECRET government computer systems.

Homeland Security Information: Any information possessed by a state, local, tribal, or federal agency that relates to a threat of terrorist activity; the ability to prevent, interdict, or disrupt terrorist activity; the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or a planned or actual response to a terrorist act.

Hypothesis: An interim conclusion regarding persons, events, and/or commodities that is formed on the basis of the accumulation and analysis of intelligence information that is to 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. Imagery 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.

Indicator: Generally defined and observable actions that, on the basis of an analysis of past known behaviors and characteristics, collectively suggest that a person may be committing, 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 related to the target.

Informant: An individual not affiliated with a law enforcement agency who provides information about criminal behavior to a law enforcement agency. An informant may be a community member, a businessperson, or a criminal informant who seeks to protect himself/herself from prosecution and/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 (ISE): The ISE provides analysts, operators and investigators with integrated and synthesized terrorism, weapons of mass destruction and homeland security information needed to enhance national security and help keep our people safe. The ISE supports the law enforcement, public safety, homeland security, intelligence, defense, and foriegn affairs communities and facilitates sharing between and among federal, state, local, tribal, and territorial governments, the private sector and foriegn partners. The ISE established by the Intelligence Reform and Terrorism Prevention Act of 2004 and the Program Manager was granted government wide authority to plan for, oversee the implementation of, and manage the ISE.

Information Sharing System: An integrated and secure methodology, whether computerized or manual, designed to efficiently and effectively distribute critical information.

Intelligence Activity: A generic term used to encompass any or all of the efforts and endeavors undertaken by intelligence organizations, including collection, analysis, production, dissemination, and covert or clandestine activities.

Intelligence Agency: A component organization of the Intelligence Community.

Intelligence Analyst: A professional intelligence officer who is responsible for performing, coordinating, or supervising the collection, analysis, and dissemination of intelligence.

Intelligence Assessment: Refers to a longer, often detailed intelligence product; encompasses most analytical studies dealing with subjects of policy significance.

Intelligence Bulletin: Refers to a shorter, often less detailed intelligence product that focuses on a particular topic or incident.

Intelligence Community: 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, Central Intelligence Agency, Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Director of National Intelligence, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, and Navy Intelligence.

Intelligence Cycle: The steps by which information is converted into intelligence and made available to users. The cycle 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 that is considered essential.

Intelligence Estimate: An 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 and/or strategic responses.

Intelligence Mission: The role that the intelligence function of an agency fulfills in support of the overall mission of the agency; it 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): JTTFs are coordinated "action arms" for federal, state, and local government response to terrorist threats in specific U.S. geographic regions. The FBI is the lead agency that overseas JTTFs.

K

Known or Suspected Terrorist: An individual "known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism."

L

Law Enforcement Sensitive (LES): Unclassified information typically originated by the 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 non-TOP SECRET computer system; can be used to refer to unclassified or SECRET-level systems.

M

Major Urban Area Fusion Center: Fusion centers located in large metropolitan areas that support the receipt and sharing of terrorism, homeland security, and law enforcement information related to terrorism. Several states maintain state-level and major urban area-level fusion centers, for example; the Commonwealth Fusion Center is Massachusetts' state fusion center, while the Boston Regional Intelligence Center (BRIC) is its major urban area fusion center.

Measurement and Signature Intelligence (MASINT): Technically derived intelligence data other than imagery and SIGINT. The data 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.

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): NCTC serves as the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the United States 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 (IT) systems and architectures within the NCTC and between the NCTC and other agencies that enable access to, as well as integration, dissemination, and use of, terrorism information.

National Intelligence Council (NIC): The NIC is the Intelligence Community's (IC) center for midterm and long-term strategic thinking. Its 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): NIEs are produced by the National Intelligence Council, express the coordinated judgments of the U.S. Intelligence Community, and thus represent the most authoritative assessment of the Director of National Intelligence (DNI) with respect to a particular national security issue. They contain the coordinated judgments of the Intelligence Community regarding the probable course of future events.

National Security: Measures adopted by the government of a nation in order to assure the safety of its citizens, guard against attack, and prevent disclosure of sensitive or classified information which might threaten or embarrass said nation.

National Security Intelligence: The collection and analysis of information concerned with the relationship and equilibrium of the United States with foreign powers, organizations, and persons regarding political and economic factors, as well as the maintenance of the United States' sovereign principles.

National Threat Advisory System (NTAS): The color-coded Homeland Security Advisory System will now be implemented as the NTAS as of April, 2011. Under the new, two-tiered system, DHS will issue formal, detailed alerts regarding information about a specific or credible terrorist threat. These alerts will include a clear statement that there is an "imminent threat" or "elevated threat." The alerts also will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals and communities can take.

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

No Fly: 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 that 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, and 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/activity and thus, deny or mitigate an adversary's/competitor's ability to compromise or interrupt said operation/activity.

P

Personally Identifiable Information: 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. This includes, but is not limited to information about an individual's education, financial transactions, and medical, criminal or employment history as well as information which can be used to distinguish or trace an individual's identity, such as his/her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., or any other information which is linked or linkable to an individual.

Plus 1: (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, SSN, 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. A policy is not a statement of what must be done in a particular situation. Rather, it is a statement of guiding principles that should be followed in activities that are directed toward the attainment of goals.

Prediction: The projection of future actions or changes in trends that is based on an analysis of information depicting historical trends from which a forecast is based.

Priority Intelligence Requirement: A prioritized informational need that is critical to mission success.

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. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records absent the written consent of the subject individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amend their records, and sets forth various agency record-keeping requirements.

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 where legal process permits use of the personally identifiable information.

Privacy (Personal): The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual, including his/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 where legal process authorizes surveillance and investigation.

Private Sector Partners: As used in the Information Sharing Environment (ISE) Implementation Plan, the term "private sector partners" includes vendors, owners, and operators of products and infrastructures participating in the ISE.

Program Manager-Information Sharing Environment: The ISE Program Manager (PM-ISE) works with mission partners - federal, state, local, tribal, and territorial governments, the private sector and foreign partners - to improve the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information. The PM-ISE facilitates the development of the ISE by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. They provide ideas, tools, and resources to mission partners and assist them in removing barriers, facilitating change, and ensuring that ISE implementation proceeds efficiently and effectively.

Consistent with the direction and policies issued by the President and the Director of the Office of Management and Budget (OMB), the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE. The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004 and the Program Manager was granted government wide authority to plan for, oversee the implementation of, and manage the ISE.

Protected Critical Infrastructure Information (PCII) Program: Enhances information sharing between the private sector and the government. The Department of Homeland Security 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 which is 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 which can be counted or placed on a scale of measurement that can be statistically analyzed.

R

Raw Data: Bits of data collected which 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 converted into finished intelligence.

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 local, state, tribal, and federal 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 the intelligence function.

Responsibility: Reflects how the authority of a unit or individual is used and determines whether goals have been accomplished and the mission fulfilled in a manner that is 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: An 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, analytical 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: 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 analytical processes that is required to 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, and/or processed.

Signals Intelligence (SIGINT): Intelligence derived from signals intercepts comprising, individually or in combination, all communications intelligence (COMINT), electronic intelligence (ELINT), and/or foreign instrumentation signals intelligence (FISINT).

Source: A book, statement, person, etc., supplying information. From an intelligence perspective, sources are persons (human intelligence or HUMINT) who collect or possess critical information needed for intelligence analysis.

Suspicious Activity Report (SAR): Per the Information Sharing Environment Functional Standard, Suspicious Activity Reporting Version 1.5, a SAR is an official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

System of Records: Pursuant to the Privacy Act of 1974, a System of Records is a group of any records under the control of any agency from which information is 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 in the Federal Register. This notice is generally referred to as a System of Records Notice (SORN).

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/recovery operations, and provide for first responder safety.

Target: (1) Any person, organization, group, crime or criminal series, or commodity being 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/her objective.

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 who are responsible.

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

Tear-line: Intelligence information which has been sanitized (removal of sources and methods) so it may be disseminated at a lower classification.

Tear-Line Report: A report containing classified intelligence or information that is prepared in such a manner that data relating to intelligence sources and methods are easily removed from the report to protect sources and methods from disclosure. Typically, the information below the "tear line" can be released as sensitive but unclassified.

Terrorism: Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.

Terrorist Identities Datamart 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 watch listing system.

Terrorist Screening Center (TSC): Established in support of Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, and led by the FBI, to consolidate the Federal Government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The TSC maintains the Federal Government's consolidated and integrated terrorist watch list, known as the Terrorist Screening Database (TSDB).

Terrorist Screening Database (TSDB): The database that contains the consolidated and integrated terrorist watch list maintained by the FBI's Terrorist Screening Center (TSC). The No Fly and Selectee Lists are components of the TSDB.

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 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.

U

Unauthorized Disclosure: A communication or physical transfer, usually of sensitive but unclassified 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.

V

Validity: Information which 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 and/or subject matter experts to ascertain the product's accuracy, consistency with philosophy, and/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 target's 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

Y

Z

109

INTELLIGENCE COMMUNITY ACRONYMS & ABBREVIATIONS

INTELLIGENCE COMMUNITY ACRONYMS & ABBREVIATIONS

The Intelligence Community makes extensive use of acronyms and abbreviations in intelligence reporting, presentations, and conversation–many are unique to this community. 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

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
AQ: al-Qa'ida
AQAP: al-Qa'ida in the Arabian Peninsula
AQI: al-Qa'ida in Iraq
AQIM: al-Qa'ida in the Islamic Maghreb [formerly Salafist Group for Preaching and Combat (GSPC)]
ATF: Bureau of Alcohol, Tobacco, and Firearms
AUC: United Self-Defense Forces of Colombia
AWN: Alerts, Warnings, and Notifications

B

BPA: Border Patrol Agent
BW: Biological Warfare

C

C: CONFIDENTIAL
CBP: U.S. Customs and Border Protection, Department of Homeland Security (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
CIS: Bureau of Citizenship and Immigration Services, DHS
CLASS: Consular Lookout and Support System
COI: Community of Interest
COMINT: Communications Intelligence
COMSEC: Communications Security
CONOPS: Concept of Operations
CONUS: Continental United States
COOP: Continuity of Operations
CT: Counterterrorism
CVI: Chemical-Terrorism Vulnerability Information

D

D/CIA: Director Central Intelligence Agency (formerly DCI)
DCI: Director of Central Intelligence [now Director of National Intelligence (DNI)]
D&D: Denial and Deception
DEA: Drug Enforcement Administration
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 [replaces Director of Central Intelligence (DCI)]
DO: Directorate of Operations, CIA (now NCS, National Clandestine Service, CIA)
DOB: Date of Birth
DOD: Department of Defense
DOE: Department of Energy
DOS: Department of State
DPOB: Date and Place of Birth
DSS: Diplomatic Security Service
DT: Domestic Terrorism

E

EAAQ: East Africa al Qa'ida
EEI: Essential Element of Information [now Priority Intelligence Requirement (PIR)]
EIF: Entry into Force
ELINT: Electronic Intelligence
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
FBIS: Foreign Broadcast Information System (now Open-Source Center)
FDO: Foreign Disclosure Officer
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 Instrumentations Intelligence
FNU: First Name Unknown
FOIA: Freedom of Information Act
FOUO: For Official Use Only
FPO: Federal Protective Service Officer
FPS: Federal Protective Service
FPU: Force Protective Unit

G

GEOINT: Geospatial Intelligence
GIA: Armed Islamic Group
GS: General Schedule
GWOT: Global War on Terror

H

HCS: Human Control System
HIR: Homeland Information Report
HITRAC: Homeland Infrastructure Threat and Risk Analysis Center, DHS
HSC: Homeland Security Council
HSDN: Homeland Secure Data Network
HSIN: Homeland Security Information Network (DHS Web portal)
HSIN-I: Homeland Security Information Network-Intelligence (DHS Web portal)
HS SLIC: Homeland Security State and Local Community of Interest
HUMINT: Human Intelligence
HUM: Harakat ul-Mujahidin

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: Inspector General
IICT: Interagency Intelligence Committee on Terrorism, National Counterterrorism Center (NCTC)
IIR: Intelligence Information Report
IJU: Islamic Jihad Union
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, DOS
INTERPOL: International Police
IRT: Incident Response Team
IRTPA: Intelligence Reform and Terrorism Prevention Act of 2004
ISC: Information Sharing Council
ISE: Information Sharing Environment
IT: International Terrorism
ITACG: Interagency Threat Assessment and Coordination Group, NCTC

J

JCS: Joint Chiefs of Staff
JEM: Jaish-e-Mohammed
JI: Jemaah Islamiya
JITF-CT: Joint Intelligence Task Force-Combating Terrorism, Defense Intelligence Agency (DIA)
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

KST: Known or Suspected Terrorist

L

LAN: Local Area Network
LEA: Law Enforcement Agency
LEO: Law Enforcement Officer
LEO: Law Enforcement Online (FBI sensitive but unclassified Web portal)
LES: Law Enforcement Sensitive
LIFG: Libya Islamic Fighting Group

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
MI: Military Intelligence
MOA: Memorandum of Agreement
MOU: Memorandum of Understanding

N

NAILS: National Automated Immigration Lookout System
NCIC: National Crime Information Center
NCIS: Naval Criminal Investigative Service
NCIX: National Counterintelligence Executive
NCPC: National Counter Proliferation Center
NCR: National Capital Region
NCS: National Clandestine Service [replaces Directorate of Operations (DO), CIA]
NCTC: National Counterterrorism Center
NFI: No Further Information
NFTR: Nothing Further to Report

NGA: National Geospatial-Intelligence Agency (formerly NIMA)
NIC: National Intelligence Council
NIE: National Intelligence Estimate
NIMA: National Imagery and Mapping Agency (now NGA)
NIO: National Intelligence Officer
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
NOC: NCTC Operations Center
NOFORN: Not Releasable to Foreign Nationals
NOIWON: National Operations and Intelligence Watch Officers Network
NOL: NCTC Online (now NCTC CURRENT)
NOL-J: NCTC Online-JWICS (now NCTC CURRENT)
NOL-S: NCTC Online-SIPRNet (now NCTC CURRENT-S)
NRO: National Reconnaissance Office
NSA: National Security Agency
NSC: National Security Council
NSEERS: National Security Entry-Exit Registration System
NSIS: National Strategy for Information Sharing
NSTL: National Security Threat List
NSTR: Nothing Significant to Report
NSTS: National Secure Telephone System
NTM: National Technical Means
NTR: Nothing to Report

O

OCONUS: Outside the Continental United States
ODNI: Office of the Director of National Intelligence
OPSEC: Operations Security
ORCON: Originator Controlled Dissemination
OSC: Open-Source Center (formerly FBIS)
OSINT: Open-Source Intelligence
OSIS: Open-Source Information System

P

PCII: Protected Critical Infrastructure Information
PII: Personally Identifiable Information
PIR: Priority Intelligence Requirement [formerly Essential Element of Information (EEI)]
PM: Production Management
PM-ISE: Program Manager-Information Sharing Environment, ODNI
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
RISS: Regional Information Sharing System
RISSNET: Regional Information Sharing System Network
RO: Reporting Officer or Reports Officer
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
SGI: Safeguards Information
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
SLAM: SIOC Law Enforcement Alert Messaging System
SLT: State, Local, and Tribal
SLTP: State, Local, Tribal, 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

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
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 & Terrorist Organization File
VTC: Video Teleconference
VWP: Visa Waiver Program

W

WMD: Weapons of Mass Destruction

X

Y

Z

NOTES

NOTES

NOTES

This document can also be found in printable format at https://hsin-intel.dhs.gov, http://www.leo.gov, or http://www.nctc.gov.














PASSPORT
United States
of America

ITACG Intelligence Guide for First Responders

11148592 | IND 06-11