



ITACG

Interagency Threat Assessment and Coordination Group

INTELLIGENCE GUIDE FOR FIRST RESPONDERS







ITACG *Interagency Threat Assessment and Coordination Group*
INTELLIGENCE GUIDE
FOR FIRST RESPONDERS



Legal Disclaimer

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

TABLE OF CONTENTS

I

GENERAL

- 1 Introduction**
- 5 What is Intelligence?**
 - 8 The Intelligence Community
 - 10 The Intelligence Cycle
 - 12 Categories of Finished Intelligence

III

HOW TO

- 17 Handling of “Controlled Unclassified Information”**
- 21 Security Clearances**
- 25 What Intelligence Can and Cannot Do**

29	Intelligence Products Typically Available to First Responders
35	Accessing Intelligence Community Products
41	Understanding Threat Information
49	Understanding Estimative Language

III

REFERENCE

55	Intelligence Community Terminology
85	Intelligence Community Acronyms and Abbreviations

ITACG: INTELLIGENCE GUIDE FOR FIRST RESPONDERS

SECTION



GENERAL



01

INTRODUCTION

INTRODUCTION

This Interagency Threat Assessment and Coordination Group (ITACG) ***Intelligence Guide for First Responders*** is designed to assist state, local, tribal law enforcement, firefighting, homeland security, and appropriate private sector personnel in accessing and understanding Federal counterterrorism, homeland security, and weapons of mass destruction intelligence reporting. Most of the information contained in this guide was compiled, derived, and adapted from existing Intelligence Community and open source references.

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



Fig.1 - Current and former members of the ITACG Detail; clockwise from the top: New Jersey State Police, Seattle Fire Department, Federal Bureau of Investigation, Boston Police Department, Illinois State Police, Phoenix Police Department (2007-2008), Six Nations Tuscarora, Las Vegas Police Department, Department of Homeland Security, DC Metropolitan Police (2008-2009)



05

WHAT IS INTELLIGENCE?

WHAT IS INTELLIGENCE?¹

"Intelligence is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity."

22 June 2007 edition of Joint Pub 2-0, Joint Intelligence

THERE ARE **SIX** BASIC INTELLIGENCE SOURCES² :

Signals Intelligence (SIGINT) is derived from the exploitation of foreign electronic emissions. SIGINT can be in the form of the actual information content of a signal or in the form of its temporal and spectral characteristics called signal operating parameters. SIGINT includes both the raw data and the analysis product of that data. SIGINT breaks down into four sub disciplines: Electronic Intelligence (ELINT), Communications Intelligence (COMINT), Foreign Instrumentation Signals Intelligence (FISINT), and weapons-related Command and Control Signals (PROFORMA).

Imagery Intelligence (IMINT) is a product that is the result of processing and exploiting raw imagery (information) and creating an analyzed product (intelligence). An image alone is only information in the form of pixels, digits, or other forms of graphic representation and the data behind that portrayal. When studied for content with an understanding of portrayal, imaging processes, and the place, objects and time captured by that process, or through comparison to other images and consideration in light of other information or intelligence, imagery intelligence (IMINT) can be created.

Measurement and Signature Intelligence (MASINT) is scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same.

Human-Source Intelligence (HUMINT) is intelligence derived from human beings who may act as both sources and collectors, and where the human is the primary collection instrument. This includes all forms of intelligence gathered by humans, from direct reconnaissance and observation to the use of recruited agents. HUMINT may also encompass interrogation techniques, including the process of questioning detainees conducted in compliance with U.S. law and regulation, international law, executive orders, and other operationally specific guidelines. HUMINT can provide a wide range of information which includes but is not limited to adversary plans and intentions, deliberations and decisions, research and development goals and strategies, doctrine, leadership, political or military relationships, weapons systems, physical and cultural infrastructure, and medical conditions. HUMINT can often collect information that is difficult or sometimes impossible to collect by other, more technical, means.

Open-Source Intelligence (OSINT) is unclassified information of potential intelligence value that is available to the general public.

Geospatial Intelligence (GEOINT) is the 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.

THE INTELLIGENCE COMMUNITY ³



"The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council 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 Intelligence Community (IC) is 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 the national security of the United States. These activities include:

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



The **Intelligence Community (IC)** refers to those agencies and organizations involved in intelligence activities: ⁴

- Air Force Intelligence
- Army Intelligence
- Central Intelligence Agency (CIA)
- Coast Guard (USCG)
- Defense Intelligence Agency (DIA)
- Department of Energy (DoE) Office of Intelligence
- Department of Homeland Security (DHS), Office of Intelligence and Analysis
- Department of State Bureau of Intelligence and Research (INR)
- Department of the Treasury (DoT), Treasury Office of Terrorism and Financial Intelligence
- Office of the Director of National Intelligence (ODNI)
- Drug Enforcement Administration (DEA), Office of National Security Intelligence
- Federal Bureau of Investigation (FBI), National Security Branch
- Marine Corps Intelligence
- National Geospatial-Intelligence Agency (NGA)
- National Reconnaissance Office (NRO)
- National Security Agency (NSA)
- Naval Intelligence

THE INTELLIGENCE CYCLE ⁵

The intelligence cycle is the process of developing raw information into finished intelligence for policymakers, military commanders, and other consumers to use in decision-making and actions.

Five steps constitute the intelligence cycle:

- 1. Planning and Direction:** Establishing the intelligence requirements of the policymakers – the President, the National Security Council, military commanders, and other officials in major departments and governmental agencies.
- 2. Collection:** Gathering of raw data from which finished intelligence is produced. There are six basic intelligence sources, or collection disciplines:
 - a. Signals Intelligence (SIGINT)
 - b. Imagery Intelligence (IMINT)
 - c. Measurement and Signature Intelligence (MASINT)
 - d. Human-Source Intelligence (HUMINT)
 - e. Open-Source Intelligence (OSINT)
 - f. Geospatial Intelligence (GEOINT)
- 3. Processing and Exploitation:** Conversion of large amounts of data to a form suitable for the production of finished intelligence; includes translations, decryption, and interpretation of information stored on film and magnetic media through the use of highly refined photographic and electronic processes.

- 4. Analysis and Production:** Integration, evaluation, and analysis of all available data and the preparation of a variety of intelligence products, including timely, single-source, event-oriented reports and longer term, all-source, finished intelligence studies.
- 5. Dissemination:** Delivering the products to consumers who request them. Some intelligence information is sent directly to consumers, usually by electronic means, because it is self-explanatory. More often, analysts check information to see how it relates to other information they have received. They evaluate the information and make comments. When information has been reviewed and correlated with information available from other sources, it is called *finished intelligence*.



CATEGORIES OF FINISHED INTELLIGENCE ⁶

There are five categories of finished intelligence available to the consumer of intelligence:

- 1. Current intelligence** addresses day-to-day events, seeking to apprise consumers of new developments and related background, to assess their significance, to warn of their near-term consequences, and to signal potentially dangerous situations in the near future. Current intelligence is presented in daily, weekly, and some monthly publications, and frequently in ad hoc written memorandums and oral briefings to senior officials.
- 2. Estimative intelligence** looks forward to assess potential developments that could affect U.S. national security. Like all kinds of intelligence, estimative intelligence starts with the available facts, but then explores the unknown, even the unknowable. Estimative intelligence helps policymakers to think strategically about long-term threats by discussing the implications of a range of possible outcomes and alternative scenarios. National Intelligence Estimates, which are estimative reports produced by the National Intelligence Council, are the Director of National Intelligence's (DNI) most authoritative written assessments of national security issues.

- 3. Warning intelligence** sounds an alarm or gives notice to policymakers. It connotes urgency and implies the potential need for policy action in response. Warning includes identifying or forecasting events that could cause the engagement of U.S. military forces, or those that would have a sudden and deleterious effect on U.S. foreign policy concerns (for example, coups, third-party wars, refugee situations). Warning analysis involves exploring alternative futures and low probability/high impact scenarios. The National Intelligence Officer (NIO) for Warning serves as the DNI's and the IC's principal adviser on warning. All agencies and intelligence staffs have designated warning components, and some have specific warning responsibilities.
- 4. Research intelligence** is presented in monographs and in-depth studies by virtually all agencies. Research underpins both current and estimative intelligence.

- 5. Scientific and technical intelligence** includes information on technical developments and characteristics, performance, and capabilities of foreign technologies including weapon systems or subsystems. This information is derived from analysis of all-source data, including technical measurements. Generally, such technical analysis and reporting responds to specific national requirements derived from the weapons acquisition process, arms control negotiations, or military operations. It covers the entire spectrum of sciences, technologies, weapon systems, and integrated operations. This type of intelligence is provided to consumers via in-depth studies, detailed system handbooks, executive summaries, focused assessments and briefs, and automated databases.

ITACG: INTELLIGENCE GUIDE FOR FIRST RESPONDERS

SECTION

II

How To

CONTRACT

RECEIVED BY THE COMPANY

By: _____
Name: _____
Title: _____
Date: _____

For contracts \$10,000 and over,
signature required.

By: _____
Name: _____
Title: Authorized Purchasing Agent
Date: _____

Contractor shall be authorized to receive payment for services rendered under this Agreement. The consideration for all services set forth on Exhibit A ("Services") shall be paid by the Company as follows:

The Contractor shall not exceed \$ _____

Contractor shall submit request for reimbursement must be itemized and accompanied by receipts. Contractor shall submit request for reimbursement must be consistent with the Company's Purchasing Services, and clearly indicate the purpose of the expense.

Contractor shall submit request for reimbursement must be consistent with the Company's Purchasing Services, and clearly indicate the purpose of the expense.

17

HANDLING OF “CONTROLLED UNCLASSIFIED INFORMATION”

HANDLING “CONTROLLED UNCLASSIFIED INFORMATION” ⁷

Controlled Unclassified Information (CUI) is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. CUI includes many caveats, such as “FOR OFFICIAL USE ONLY” (FOUO).

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. ⁸

FOUO is not a classification, but a dissemination control marking. It is 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.

Dissemination of FOUO is 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 to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties. Typical FOUO requirements include:

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

Many government agencies use the FOUO caveat, but other caveats, such as, LAW ENFORCEMENT SENSITIVE (LES), and OFFICIAL USE ONLY (OUO), are also used. In many instances the requirement for safeguarding this information is equivalent; however, these agencies may have additional requirements concerning the safeguarding of sensitive information.



CANCEL

ANNULER

QZ
1

ABC
2

DEF
3

GHI
4

JKL
5

MNO
6

OK

DECIMAL
POINT
DECIMAL

21

SECURITY CLEARANCES

SECURITY CLEARANCES ⁹

Most information needed by state, local, and tribal first responders can be shared at an unclassified level. In those 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 process involves completing a Questionnaire for National Security Positions, submitting fingerprints, and undergoing a background investigation.

Records checks for Secret and Top Secret security clearance are mandated by Presidential Executive Order (EO). The EO requires these procedures in order for a security clearance to be granted and they cannot be waived.

- 1. Secret Clearances:** A Secret security clearance may be granted to those persons 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.

- 2. Top Secret Clearances:** A Top Secret clearance may be granted to those persons who “need-to-know” national security information, classified up to the Top Secret level, and who need unescorted access to sensitive facilities, when necessary.
- a. In addition to all the requirements at the Secret level, a background investigation, covering a 10-year time period, is required.
 - b. Once favorably adjudicated for a Top Secret security clearance, the candidate will be required to sign a Non-Disclosure Agreement.

For additional information, visit <http://www.fbi.gov/clearance/securityclearance.htm> or contact your local FBI Field Office.



25

WHAT INTELLIGENCE CAN AND CANNOT DO

WHAT INTELLIGENCE CAN (AND CANNOT) DO ¹⁰

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 information can provide valuable services, such as:

- Providing decision advantage, by improving the decision-making of 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.
- Assistance in preparation for senior-level meetings that include national security-related subjects.
- Pre-travel security overviews and support.
- Reports on specific topics, either as part of ongoing reporting or upon request for short-term needs.
- Compiling U.S. Government knowledge on persons of interest.

2. WHAT INTELLIGENCE CANNOT do: Realistic expectations will help the consumer fill their intelligence needs. Some things that intelligence cannot do include:

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



29

INTELLIGENCE PRODUCTS TYPICALLY AVAILABLE TO FIRST RESPONDERS

INTELLIGENCE PRODUCTS TYPICALLY AVAILABLE TO FIRST RESPONDERS ¹¹

The following types of products can be found on a variety of classified and unclassified systems, including FBI's Law Enforcement Online (LEO), and DHS's Homeland Secure Information Network-Intelligence (HSIN-I) via the Internet, and NCTC Online-SECRET (NOL-S) via secret level systems, such as FBI Network (FBINet), Homeland Secure Data Network (HSDN), Joint Deployable Intelligence Support System (JDISS), and Secure Internet Protocol Routed Network (SIPRNet).

- 1. Situational Awareness and Threat Reporting:** These are breaking news events to chief executives and command centers with state, local, and tribal law enforcement agencies via HSIN-I, LEO, text messaging, or e-mail. These reports are often produced jointly by DHS and FBI.
- 2. Information Report:** These are specially formatted messages transmitted electronically, which enable the timely dissemination of unevaluated intelligence within the Intelligence Community and law enforcement. The information conveyed in these products may be non-specific or fragmentary and simply constitute suspicious activity, but still be of intelligence value. These products include:
 - a. IIR (Intelligence Information Report)
 - b. HIR (Homeland Information Report)

3. **Intelligence Assessment (IA):** Finished intelligence products resulting from the intelligence analysis process. Assessments may address tactical, strategic, or technical intelligence requirements.
4. **Threat Assessment (TA) or Special Assessment (SA):** Provides in-depth analysis related to a specific event or body of threat reporting.
5. **Intelligence Bulletin (IB):** 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. An IB does not address threat warning information.
6. **Joint Intelligence Assessment (IA) or Intelligence Bulletin (IB):** Assessments or bulletins which are written jointly by two or more IC agencies (dual or multiple seals). These products may address the same types of requirements as Intelligence Assessments or Intelligence Bulletins. These joint products may be formatted differently than single seal versions, depending on the format agreed to by participating agencies.

7. **Other Reports:** These include intelligence summaries and briefs produced daily, which cover current counterterrorism, homeland security, and WMD-related information. Examples include:
- a. **Roll Call Release:** The Roll Call Release is a collaborative FOUO-only product developed by DHS, FBI, and the ITACG. The product is written specifically for state, local, and tribal first responders, and focuses on terrorist tactics, techniques, procedures; terrorism trends; and indicators of suspicious activity. The product is written on an ad hoc basis, is focused on one subject, and fits on one page. These products are posted on HSIN-I and LEO.
 - b. **Terrorism Summary (TERRSUM):** The TERRSUM is a SECRET collateral 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 posted on NOL-S.

NOTES

This image shows a single sheet of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. There are approximately 20 lines visible. The paper appears to be a standard notebook page or a sheet of stationery.



35

ACCESSING INTELLIGENCE COMMUNITY PRODUCTS

ACCESSING INTELLIGENCE COMMUNITY PRODUCTS ¹²

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

1. UNCLASSIFIED INTELLIGENCE PRODUCTS

a. **Homeland Security Information Network – Intelligence (HSIN-I):**

HSIN-I is an official government information sharing and electronic communications portal. It provides DHS, FBI, NCTC, other federal and non-federal intelligence products at the FOUO level. Accounts are available to federal, state, local, and tribal personnel performing homeland security or law enforcement duties. HSIN-I can be accessed from any computer system with an Internet connection. Access is by invitation only.

- i. Website: <https://hsin-intel.dhs.gov>
- ii. Access: Contact the helpdesk at 1-877-624-3771 or e-mail hsin.intel@hq.dhs.gov for sponsor contact information. Sponsors for state, local, and tribal can be contacted through the State and Local Fusion Centers.

- b. **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 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.
 - i. Website: <http://www.leo.gov>
 - ii. Access: Go to <http://www.leo.gov>, click on the “LEO Membership Criteria” and then click on the “LEO User Application”, or contact LEO Helpdesk at 1-888-334-4536, or e-mail helpdesk@leo.gov.
- c. **Intelink-U:** Intelink-U is the Intelligence Community’s “Sensitive but Unclassified” (SBU) information sharing network. Content is provided by the Intelligence Community, 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.
 - i. Website: <https://www.intelink.gov>
 - ii. Access: Go to <https://www.intelink.gov>, click on “Sign In”, and proceed to “New Account Registration”.
- d. **Regional Information Sharing Systems Network (RISSNET):** RISSNET facilitates information sharing within the law enforcement community to combat multi-jurisdictional criminal activities and conspiracies. It is composed of six multi-state intelligence centers (RISS Intelligence Centers). Membership comprises federal, state, local, and tribal law enforcement agencies. Access is requested through the regional RISS Intelligence Centers.

- i. Website: <http://www.riss.net>
 - ii. Contact information available at <http://www.riss.net/Centers.aspx>.
- e. **DHS Technical Resources for Incident Prevention (TRIPwire):** TRIPwire is a secure information sharing network for law enforcement, bomb squads, and other first responders. Content consists of current terrorist bombing tactics, techniques, and procedures.
 - i. Website: <https://www.tripwire-dhs.net>
 - ii. Access: Apply online at <https://www.tripwire-dhs.net>.
- f. **Federal Protective Service Portal (FPS Portal):** The FPS Portal is a compilation of FOUO products for law enforcement and first responders.
 - i. Website: <https://fps.esportals.net>
 - ii. Access: For membership contact helpdesk@espgroup.net or 877-624-3771.
- g. **Open Source Center (OSC):** OSC contains open source reporting, analysis, and translations of foreign policy and national security issues. Accounts are available to individuals with federal, state, and local homeland security and counterterrorism responsibilities.
 - i. Website: <http://www.opensource.gov>
 - ii. Access: Apply online at <http://www.opensource.gov>.

2. SECRET INTELLIGENCE PRODUCTS

- a. **NCTC Online-SECRET (NOL-S)**: NOL-S can be accessed from any SECRET U.S. Government information system (HSDN, FBINet, JDISS, or SIPRNet).
 - i. Website: <https://nol.nctc.sgov.gov>
 - ii. Access: Authorized access to HSDN, FBINet, JDISS, or SIPRNet is the only requirement.

- b. **Office of Intelligence and Analysis (OI&A) Webpage, DHS**: The OI&A homepage can be accessed from any SECRET U.S. Government information system (HSDN, FBINet, JDISS, or SIPRNet).
 - i. Website: <http://dhs.csp.sgov.gov>
 - ii. Access: Authorized access to HSDN, FBINet, JDISS, or SIPRNet is the only requirement.

- c. **FBINet**: The FBI intranet can only be accessed from an FBINet computer.
 - i. Website: <http://intranet.fbinet.fbi>
 - ii. Access: Authorized access to an FBINet system.

- d. **FBI Intelink/SIPRNet**: Can be accessed from any SECRET U.S. Government information system (HSDN, FBINet, JDISS, or SIPRNet).
 - i. Website: <http://www.fbi.sgov.gov>
 - ii. Access: Authorized access to HSDN, FBINet, JDISS, or SIPRNET is the only requirement.



41

UNDERSTANDING THREAT INFORMATION

UNDERSTANDING THREAT INFORMATION¹³

A raw intelligence report, alert, warning, or notification is a message that 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. The information may be nonspecific or fragmentary and simply constitute suspicious activity but still be of intelligence value.

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

a. **Access:** Addresses the ability of the source to obtain the information. Some common levels of source access are:

- i. **Direct Access:** The intelligence source has direct knowledge of the intelligence fact reported or appears to be in the direct contact with those personally involved or knowledgeable.
- ii. **Indirect Access:** Some distance between the source and origin of the information. The intelligence source is reporting information obtained at one or more steps removed from those with first-hand knowledge.

- iii. **Excellent Access:** High-level access to information due to the source's involvement in the event; source may have learned the information from the decision maker or from a source document.
 - iv. **Good Access:** Suggests credible but no direct access to the information. Perhaps the source obtained the information from a sub-source with excellent access or from a sub-source with a proven reporting record.
- b. **Chain of Acquisition:** Addresses source relationships and potential changes in the information as it passes 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, affecting the accuracy of the information.
- c. **Credibility:** 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 just 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 sensor may be more credible regarding certain events and at certain times but not so credible regarding other events or at other times.

- d. **Reliability:** A criteria 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 based on the past performance of the source. An analyst's judgment on the intelligence source for a particular report.
- i. **Reliable:** Established reporting record judged to be accurate.
 - i. "Source has reported reliably in the past"
 - ii. "Source has reported reliably over 1-10+ years"
 - ii. **Uncertain:** Limited reporting record and/or some uncertainty as to the reliability of the source or sources: "Reporting reliability cannot be confirmed."
 - iii. **Unknown:** Previously unreported source.



2. SOURCE CATEGORIES: The Intelligence Community assesses the source of the information to assist in understanding threat information. The following terms are commonly used in describing sources:

- a. **Contact:** Unilateral contacts who provide information voluntarily and in confidence, but for whom a formal relationship has not been established: “A contact with (*direct/indirect/good/excellent*) access who spoke in confidence. This is the first reporting from source, reliability cannot be determined.”
- b. **Collaborative Source:** Newly established sources with whom a formal relationship has recently been established. The reliability statement is based on a combination of the quantity and quality of the source’s reporting: “A collaborative source with (*direct/indirect/good/excellent*) access (*some/much/all*) of who’s reporting has been corroborated over the past two years.”
- c. **Established Source:** Sources with which a relationship has been established and, if revealed, would possibly endanger his/her status, reputation, or security. The reliability statement is based on a combination of the quantity and quality of the source’s reporting: “An established source with (*direct/indirect/good/excellent*) access (*some/much/all*) of who’s reporting has been corroborated over the past two years.”

- d. **Walk-in/Call-in/Write-in:** A previously unknown individual who makes contact with an official U.S. person, installation, or website and volunteers his/her information, with or without requesting some form of assistance in return. Examples:
- i. “A write-in to an official U.S. Government website. The information was conveyed in writing, via email or other form of correspondence.”
 - ii. “A write-in to an official government agency. The information was conveyed in writing, via email or other form of correspondence.”
 - iii. “A walk-in to an official government agency. The information was conveyed in a face-to-face manner.”
 - iv. “A call-in to an official government agency. The information was conveyed telephonically.”
- e. **Sensitive Source:** A source, which if compromised, might reduce the ability to use the source in support of future collection activities: “A sensitive source with excellent access.”

3. ADDITIONAL SOURCE STATEMENT EXAMPLES:

- a. "Source obtained the information from a reliable sub-source with direct access."
- b. "Source obtained the information from a sub-source whose reporting record has not been established."
- c. "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."
- d. "The veracity of this source's information is seriously doubted but is being reported here because of the nature of the threat discussed."
- e. "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."
- f. "The information provided in this report may have been intended to influence as well as to inform."



49

UNDERSTANDING ESTIMATIVE LANGUAGE

UNDERSTANDING ESTIMATIVE LANGUAGE¹⁴

When the Intelligence Community uses words such as “we judge” or “we assess”—terms that are used synonymously—as well as “we estimate,” “likely” or “indicate,” the Intelligence Community 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 Intelligence Community 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 Intelligence Community 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 Intelligence Community 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 Intelligence Community 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 Intelligence Community also ascribes “high,” “moderate,” or “low” confidence levels based on the scope and quality of information supporting its judgments.

1. **“HIGH CONFIDENCE”** generally indicates that the Intelligence Community’s judgments are based on high-quality information and/or that the nature of the issue makes it possible to render a solid judgment.
2. **“MODERATE CONFIDENCE”** generally means that the information is interpreted in various ways, that the Intelligence Community has alternative views, or that the information is credible and plausible but not corroborated sufficiently to warrant a higher level of confidence.
3. **“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 Intelligence Community has significant concerns or problems with the sources.

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

ITACG: INTELLIGENCE GUIDE FOR FIRST RESPONDERS

SECTION

III

REFERENCE

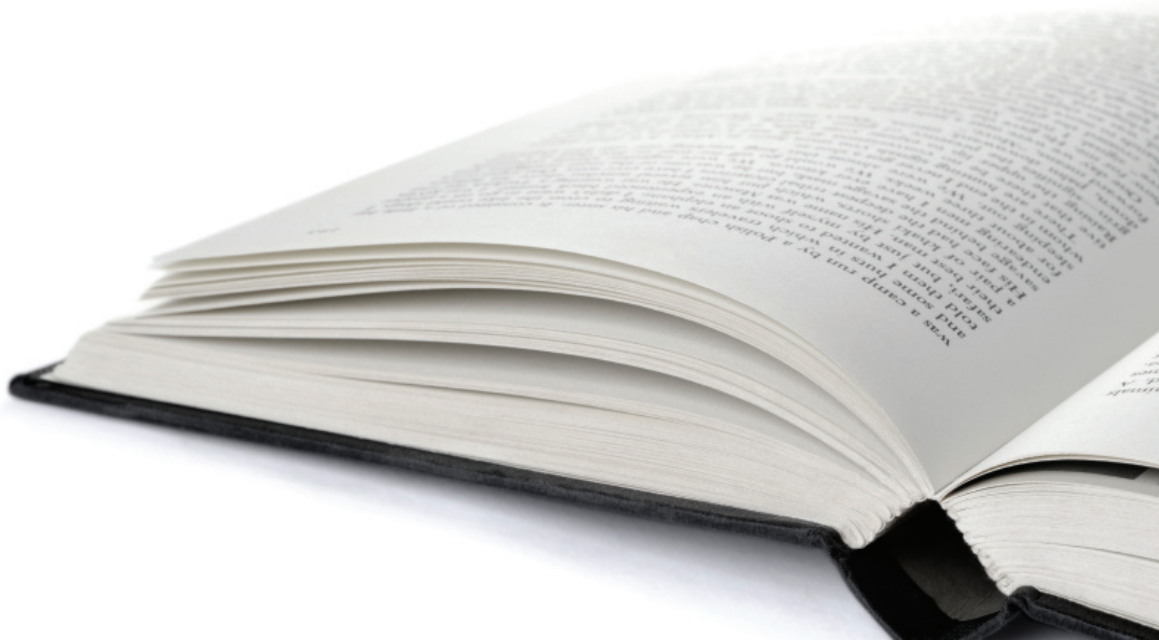


55

INTELLIGENCE COMMUNITY TERMINOLOGY

INTELLIGENCE COMMUNITY TERMINOLOGY ¹⁵

The following terminology is not exhaustive, but 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 our intended audience.



A

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, close support of US negotiating teams, or action elements dealing with such matters as international terrorism or narcotics. (2) Intelligence and information with sufficient specificity and detail that explicit responses to prevent a crime or terrorist attack can be implemented.

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

All-Source Intelligence: Intelligence information derived from any or all of the intelligence disciplines, including SIGINT, HUMINT, IMINT, 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: Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries and areas that may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject.

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.

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.

Conclusion: A definitive statement about a suspect, action, or state of nature based on the analysis of information.

Confidential: Information which if made public could be expected to cause damage to national security.

Consumer: The user of finished intelligence.

Coordination: The process of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment.

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: Offensive measures taken to prevent, deter, and respond to a terrorist act, or the documented threat of such an act.

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 not customarily in the public domain and 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 deal with the development of “codes” and the “scrambling” of communications in order 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 process of effectively distributing analyzed intelligence utilizing certain protocols in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals.

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

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

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 in order to identify and appraise such factors as available and needed assets, potential obstacles, accomplishments, and consequences.

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 a Federal Bureau of Investigation field office that is responsible for the management, execution, and coordination of intelligence functions within the field office region.

Finished Intelligence: (1) The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. (2) The final result of the production step of the intelligence cycle; the intelligence product.

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

For Official Use Only (FOUO): A dissemination control marking used to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely 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: The place where law enforcement, public safety, and private sector partners can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity. A collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorism activity.

G

Geospatial: Describes any data containing coordinates defining a location on the earth's surface.

Geospatial Intelligence: Describes the combination of spatial software and analytical methods with terrestrial and geographic datasets (imagery and geodetic, terrain elevation, hydrographic, topographic, and aeronautical data). The analysis and visual representation of security related activities on the earth.

Granularity: Considers the specific details and pieces of information, including nuances and situational inferences, which constitute the elements on which intelligence is developed through analysis.

H

Highside: Jargon for top secret government computer systems.

Homeland Security Advisory System: Designed to guide DHS protective measures when specific information to a particular sector or geographic region is received. It combines threat information with vulnerability assessments and provides communications to public safety officials and the public. The system includes:

- **Homeland Security Threat Advisories** contain actionable information about an incident involving, or a threat targeting, critical national networks, infrastructures, or key assets.
- **Homeland Security Information Bulletins** communicate information of interest to the nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of warning messages.
- **Color-coded Threat Level System** is used to communicate with public safety officials and the public at-large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood or impact of an attack. There are five levels: **Low**, **Guarded**, **Elevated**, **High**, and **Severe**.

Hypothesis (from Criminal Intelligence Analysis): An interim conclusion regarding persons, events, and/or commodities based on the accumulation and analysis of intelligence information that is to be proven or disproved 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): Those 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, based on 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 taking diverse pieces of specific information and inferring a broader meaning of the information through the course of hypothesis development.

Inference Development: The creation of a probabilistic conclusion, estimate, or prediction related to an intelligence target based upon the use of 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 a criminal event or witnesses or evidence of a criminal event.

Information Sharing Environment: As stated in the *Information Sharing Environment Implementation Plan*, “information sharing environment” and “ISE” mean an approach that facilitates the sharing of terrorism information. [IRTPA 1016(a)(2)] The ISE is to provide and facilitate the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. [Extracted from IRTPA 1016(b)(2)] To the greatest extent practicable, the ISE is to provide the functional equivalent of or otherwise support a decentralized, distributed, and coordinated environment.

Information Sharing System: An integrated and secure methodology, whether computerized or manual, designed to efficiently and effectively distribute critical information about offenders, crimes, and/or events in order to enhance prevention and apprehension activities by law enforcement.

Intelligence Analyst: A professional position in which the incumbent is responsible for taking the varied facts, documentation of circumstances, evidence, interviews, and any other material related to a crime and organizing them into a logical and related framework for the purposes of developing a criminal case, explaining a criminal phenomenon, describing crime and crime trends and/or preparing materials for court and prosecution, or arriving at an assessment of a crime problem or crime group.

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 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 the national security of the U.S.. 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 and exploitation; analysis and production; and dissemination.

Intelligence Information: Unevaluated material that may be used in the production of intelligence.

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

Intelligence Bulletin: Refers to shorter, often less detailed intelligence products which focus on a particular incident.

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.

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 decision making 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.

Intelligence Officer: A professional employee of an intelligence organization.

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, upon which there is a need for the collection of intelligence information or the production of intelligence.

J

Joint Regional Information Exchange System (JRIES): A subscriber-supported analytical and resource system for local, state, and federal law enforcement, with an interface to the U.S. Department of Defense, that provides secure sensitive but unclassified real-time information with databases, e-mail, media studies, threat reporting, analytic tools, and mapping and imagery tools.

K

Known or Suspected Terrorist: Pursuant to Homeland Security Presidential Directive 6 (HSPD-6), a known or suspected terrorist is 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 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: Jargon for *non*-top secret computer system; can be used to refer to unclassified or secret-level systems.

M

Measurement and Signature Intelligence (MASINT): Technically derived intelligence data other than imagery and SIGINT. 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 (e.g., 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 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 with regard to political and economic factors, as well as the maintenance of the United States' sovereign principles.

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 allowed on commercial flights due to terrorism concerns.

No-Fly List: A list created and maintained by the U.S. Government to keep known or suspected terrorists off commercial flights.

O

Open Source: Information of potential intelligence value that is available to the general public.

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.

Operational Intelligence: Information is evaluated and systematically organized on an active or potential target, such as groups of or individual criminals, relevant premises, contact points, and methods of communication. This process is developmental in nature wherein there are sufficient articulated reasons to suspect criminal activity. Intelligence activities explore the basis of those reasons and newly developed information in order to develop a case for arrest or indictment.

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. "Individual" includes, but is not limited to, U.S. citizens, legal permanent residents, and visitors to the U.S. "Information" includes any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. [*See Executive Office of the President, Office of Management and Budget, July 12, 2006, M-06-19*].

Plus 1: (1) One additional of something. (2) An individual's name plus an additional data element (e.g., 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 which are directed toward the attainment of goals.

Prediction: The projection of future actions or changes in trends 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 (Information): The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by criminal justice agencies, 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 criminal justice agencies, with use of such information to be strictly limited to circumstances where legal process authorizes surveillance and investigation.

Privacy Act: The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. 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 amendment of their records, and sets forth various agency record-keeping requirements.

Private Sector Partners: As used in the ISE Implementation Plan, “private sector partners” includes vendors, owners, and operators of products and infrastructures participating in the ISE.

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 types of intelligence operational law enforcement elements need from the intelligence function within an agency or other intelligence-producing organizations in order for law enforcement officers to maximize protection and preventive efforts as well as identify and arrest persons who are criminally liable.

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: Defined as the potential for undesirable outcomes for a given situation or problem.

Risk Assessment: An analysis of a target, illegal commodity, or victim to identify the probability of being attacked or criminally compromised and to analyze vulnerabilities.



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 in order to permit wider dissemination.

Secret: Information which 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 which pertains to significant law enforcement cases under investigation and criminal intelligence reports which require dissemination criteria 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 signal 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, these are persons (human intelligence or HUMINT) who collect or possess critical information needed for intelligence analysis.

Suspicious Activity Report (SAR): The reporting of suspicious activity to an appropriate government agency, defined as behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal espionage, or other illicit intention.

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: Evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case.

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 which an adversary has determined possesses information that might prove useful in attaining his/her objective.

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

Targeting: The identification of crimes, crime trends, and crime patterns that have discernable characteristics which make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible.

Tear-line: Intelligence information which has been sanitized (removal of sources and methods) in order to distribute this information 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 sub-national groups or clandestine agents, usually intended to influence an audience. Title 22, U.S.C. Section 265f (d)

Terrorist Screening Center (TSC): Established in support of Homeland Security Presidential Directive 6 (HSPD-6), dated September 16, 2003, 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 TSDB.

Terrorist Screening Database (TSDB): The database which contains the consolidated and integrated terrorist watch list maintained by the Federal Bureau of Investigation's Terrorist Screening Center (TSC). The No Fly and Selectee List 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) The capability of an adversary coupled with his intentions to undertake any action detrimental to the interests of the United States. (2) A source of unacceptable risk.

Threat Assessment: An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal's or terrorist's opportunity, capability, and willingness to fulfill the threat.

Top Secret: Information which if made public could be expected to cause exceptionally grave damage to national security.

U

Unauthorized Disclosure: A communication or physical transfer to an unauthorized recipient.

Unclassified: Information not subject to a security classification, i.e., information not CONFIDENTIAL, SECRET or TOP SECRET. Although Unclassified information is not subject to security classification, there may be limits on disclosure. (See Section 8. Handling of “Controlled Unclassified Information.”)

V

Validity: 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 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: Susceptibility to attack, exploitation, or injury; an inherent weakness or flaw. One of three key aspects of determining risk: vulnerability, threat, and impact.

Vulnerability Assessment: An assessment of possible criminal or terrorist group 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

NOTES

[illegible]



85

INTELLIGENCE COMMUNITY ACRONYMS & ABBREVIATIONS

INTELLIGENCE COMMUNITY ACRONYMS & ABBREVIATIONS ¹⁶

The following list is not exhaustive, but contains the acronyms and abbreviations which are likely to be encountered by first responders reading intelligence material.



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
ANW: Alerts, Notifications, and Warnings
AQ: al-Qa'ida
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

B

BPA: Border Patrol Agent
BW: Biological Warfare

C

C: Confidential
CBP: U.S. Customs and Border Protection, DHS
CBR: Chemical, Biological and Radiological
CBRN: Chemical, Biological, Radiological and Nuclear
CBRNE: Chemical, Biological, Radiological, Nuclear and Explosives

CBT: Computer-Based Training
CBW: Chemical and Biological Warfare
CDD: Chemical Dispersion Device
CI: Counterintelligence
CI Poly: Counterintelligence Polygraph
CIA: Central Intelligence Agency
CIR: Central Intelligence Report
CIR: Counterintelligence Report
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 U.S.
COOP: Continuity of Operations
CT: Counterterrorism
CTC: Counterterrorism Center
CUI: Controlled Unclassified 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

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))
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

EEAQ: East Africa al Qa'ida
EI: Essential Element of Information (now 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)
FCPO: Fusion Center Program Office
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
FNU: First Name Unknown
FPO: Federal Protective Service Officer
FOIA: Freedom of Information Act
FOUO: For Official Use Only
FPS: Federal Protective Service
FPU: Force Protective Unit

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 Intelligence Community of Interest

HUMINT: Human Intelligence

HUM: Harakat ul-Mujahidin

I

I&W: Indications and Warning

IA: Intelligence Assessment

IA: Intelligence Analyst

IAEA: International Atomic Energy Agency

IBIS: Interagency Border Inspection System

IC: Intelligence Community

ICD: Improvised Chemical Device

ICD: Intelligence Community Directive (replaces Director of Central Intelligence Directives, or DCIDs)

ICCD: Improvised Chemical Dispersion Device

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, 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, 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**L**

LAN: Local Area Network
LEA: Law Enforcement Agency
LEO: Law Enforcement Officer
LEO: Law Enforcement Online (FBI UNCLASS 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 the 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

NAIS: National Automated Immigration Lookout System
NIE: National Intelligence Estimate
NCIC: National Crime Information Center
NCIS: Naval Criminal Investigative Service
NCIX: National Counterintelligence Executive
NCPC: National Counter Proliferation Center
NCR: National Capital Region
NCTC: National Counterterrorism Center
NFI: No Further Information
NGA: National Geospatial-Intelligence Agency (formerly NIMA)
NIC: National Intelligence Council
NIE: National Intelligence Estimate
NIO: National Intelligence Officer
NIP: National Intelligence Program
NIPF: National Intelligence Priorities Framework
NIMA: National Imagery and Mapping Agency (now NGA)
NJTTF: National Joint Terrorism Task Force
NLETS: National Law Enforcement Telecommunication System
NOC: National Operations Center, DHS
NOFORN: Not Releasable to Foreign Nationals
NOIWON: National Operations and Intelligence Watch Officers Network
NOL: NCTC Online
NOL-J: NCTC Online-JWICS
NOL-S: NCTC Online-SIPRNET (also NCTC Online-Secret)
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
OI&A: Office of Intelligence & Analysis, DHS
OPSEC: Operations Security
ORCON: Originator Controlled Dissemination
OSC: Open Source Center (formerly FBIS)
OSINT: Open Source Intelligence
OSIS: Open Source Information System

P

PIR: Priority Intelligence Requirement (formerly EEI)
PM-ISE: Program Manager-Information Sharing Environment
POB: Place of Birth
POC: Point of Contact
POE: Port of Entry

PM: Production Management
PNR: Passenger Name Record
PPN: Passport Number
PSA: Protective Security Advisor, DHS

Q

QJBR: al-Qa'ida in Iraq (Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn)

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
RSO: Regional Security Office or Officer

S

S: Secret
S&T: Science & Technology
S&L: State and Local
SA: Situational Awareness
SA: Special Assessment
SAP: Special Access Program

SAR: Suspicious Activity Report
SBI: Special Background Investigation
SBU: Sensitive But Unclassified
SCI: Sensitive Compartmented Information
SCIF: Sensitive Compartmented Information Facility
SEG: Special Events Group
SES: Senior Executive Service
SETA: Special Events Threat Assessment
SEVIS: Student Exchange Visitor Information System
SI: Sensitive Information
SI: Special Intelligence
SIA: Supervisory Intelligence Analyst
SIO: Supervisory Intelligence Officer
SIOC: Strategic Information and Operations Center, FBI
SIPRNET: Secret Internet Protocol Routed Network
SIS: Senior Intelligence Service
SNIS: Senior National Intelligence Service
SOP: Standard Operating Procedure
SLAM: SIOC Law Enforcement Alert Messaging
STE: Secure Telephone
SLFC: State and Local Fusion Center
SLT: State, Local, and Tribal
SLTP: State, Local, Tribal, and Private Sector
STU III: Secure Telephone Unit III
SSI: Sensitive Security Information
SSO: Special Security Officer
SME: Subject Matter Expert
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 Data Mart Environment
TLO: Terrorism Liaison Officer
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
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
VWI: Virtual Walk-In
VWP: Visa Waiver Program

W

WMD: Weapons of Mass Destruction

X**Y****Z**

END NOTES

- ¹ <http://www.intelink.ic.gov/wiki/Intelligence>
- ² http://www.intelink.ic.gov/wiki/Intelligence_Sources_and_Methods
- ³ <http://www.intelligence.gov/1who.shtml>
- ⁴ http://www.intelink.ic.gov/wiki/Intelligence_community
- ⁵ <http://www.intelligence.gov/2-business.shtml>
- ⁶ <http://www.intelligence.gov/2-business.shtml>
- ⁷ <http://www.archives.gov/cui/>
- ⁸ DHS MD 11042.1
- ⁹ <http://www.fbi.gov/clearance/securityclearance.htm>
- ¹⁰ 2009 National Intelligence – a consumer’s guide; http://www.intelink.ic.gov/wiki/Intelligence_Community_Customer_Handbook
- ¹¹ Multiple Sources
- ¹² Multiple Sources
- ¹³ FBI Intelligence Information Report (IIR) Handbook, 10/23/2006
- ¹⁴ What We Mean When We Say: An Explanation of Estimative Language
- ¹⁵ Multiple Sources
- ¹⁶ Multiple Sources

NOTES

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

NOTES

This image shows a single sheet of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. There are approximately 20 lines visible. The paper has a slight shadow on the right side, suggesting it's resting on a surface.

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





ITACG INTELLIGENCE GUIDE FOR FIRST RESPONDERS

