

2014 National Network of Fusion Centers Final Report: Glossary

The following terms were used for the purposes of the 2014 Fusion Center Assessment and 2014 National Network of Fusion Centers Final Report.

28 CFR Part 23—28 Code of Federal Regulations (CFR) Part 23 is a regulation and guideline for law enforcement agencies. It contains implementing standards for operating multijurisdictional criminal intelligence systems receiving federal grant funding. It specifically provides guidance in five primary areas: (1) submission and entry of criminal intelligence information, (2) security, (3) inquiry, (4) dissemination, and (5) the review-and-purge process. This regulation also helps ensure the protection of the privacy, civil rights, and civil liberties of individuals during the collection and exchange of intelligence information.

-A-

Advisory Board—An entity that provides advice and counsel to a Fusion Center Director and/or a fusion center governance body; it does not typically have oversight responsibilities.

All-Crimes—An approach that incorporates terrorism and other high-risk threats into the existing crime-fighting framework to ensure that possible precursor crimes are screened and analyzed for linkages to larger-scale terrorist or other crimes. This approach recognizes that there is a nexus between types of criminal activity (for example, illegal drug operations, gangs, money laundering, fraud, identity theft, and terrorism). Using an all-crimes approach does not imply that a fusion center must address every single crime that occurs within its area of responsibility. Rather, the routine risk assessment that a fusion center develops or supports development of should assist in prioritizing which crimes and/or hazards a state or region should address and, in the development of a collection plan, identify what other sources of information may be useful for examining possible connections with other crimes.

All-Hazards—Refers to preparedness for terrorist attacks, major disasters, and other emergencies within the United States. Within the context of the fusion process, some fusion centers have defined their mission to include an all-hazards approach. While the application of

this approach varies, in general, it means that the fusion center has identified and prioritized types of major disasters and emergencies, beyond terrorism and crime, that could occur within their jurisdiction and gathers, analyzes, and disseminates information which would assist the relevant responsible agencies (law enforcement, fire, public health, emergency management, critical infrastructure, etc.) with the prevention, protection, response, or recovery efforts of those incidents.

Analysis—An activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.

Analytic Personnel—Fusion center personnel whose primary role is to conduct analysis or the research, writing, and review of information and/or intelligence products. All fusion center analytic personnel must meet designated competencies, as identified in the *Common Competencies for State, Local, and Tribal Intelligence Analysts*, that have been acquired through experience or training courses and must have successfully completed training to ensure baseline proficiency in intelligence analysis and production and/or previously served as an intelligence analyst for a minimum of two years in a federal intelligence agency, the military, or a state and/or local law enforcement intelligence unit.

Analytic Product (may also be called Intelligence Product)—A report or document that contains assessments, forecasts, associations, links, and/or other outputs from the analytic process that may be disseminated for use in the improvement of preparedness postures, risk mitigation, crime prevention, target hardening, or apprehension of offenders, among other activities. Analytic products may be created or developed jointly with federal, state, and local partners.

Analytic Production Plan—A document that describes the types of analysis and products a fusion center intends to provide for customers and partners, how often or in what circumstances the products will be produced, and how each product type will be disseminated.

Anti-Terrorism Advisory Council (ATAC)—Groups of law enforcement and other officials, chaired by U.S. Attorneys, that promote information sharing, provide training, coordinate the overall anti-terrorism mission, work closely with the Joint Terrorism Task Force, and prosecute any terrorist or terrorism-related cases.

Approved Plan, Policy, or SOP—A documented plan, policy, or standard operating procedure (SOP) that has been approved by a fusion center's approval authority, as required by a fusion center's approval process. The plan, policy, or SOP may be further revised or updated (e.g., some centers view their plans, policies, or SOPs as living documents that are continually subject to updates), but in its current state, the plan, policy, or SOP is approved as a final document.

Area Maritime Security Committee (AMSC)—The AMSC brings together appropriately experienced representatives from a variety of sources in a port, led by the U.S. Coast Guard, to continually assess security risks and determine appropriate risk mitigation strategies and to develop, revise, and implement security plans.

-B-

Building Communities of Trust—Initiative focused on developing relationships of trust among police, fusion centers, and the communities they serve to address the challenges of crime and terrorism prevention.

-C-

Colocation—Two or more organizations operating in the same building or office space.

Communications Plan—A plan to enhance awareness of the fusion center's purpose, mission, and functions with leaders and policymakers, the public sector, the private sector, the media, and citizens. A communications plan can help fusion centers define customers and stakeholder groups, outline key messages, and organize outreach and engagement activities to achieve intended communications objectives.

Concept of Operations (CONOPS)—A document that provides an overview of a program or system. For example, a CONOPS would usually include the program's mission, goals, and objectives. A CONOPS might also include roles and responsibilities of the program's key stakeholders and the high-level processes to achieve program goals and objectives.

Conduct—To lead or direct the performance or implementation of an activity (e.g., to conduct a threat assessment).

Consequence—The effect of an event, incident, or occurrence. The *2009 National Infrastructure Protection Plan* divides consequences into four main categories: public health and safety, economic, psychological, and governance impacts.

Consequence Analysis or Assessment—Product or process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence.

Contribute—To play a part in the planning or execution of an activity (e.g., to contribute analysis or intelligence that supports the development of a threat assessment).

Coordinating Body—The entity primarily responsible for organizing and directing a specific activity with multiple stakeholders or participants.

Countering Violent Extremism (CVE)—An approach to mitigating or preventing potential terrorist activity that emphasizes the strength of local communities via engagement with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators associated with terrorist activity.

Counterterrorism—Practices, tactics, techniques, and strategies designed to prevent, deter, and respond to terrorism. Within the context of the fusion process, a fusion center with a counterterrorism mission is one that identifies and prioritizes potential terrorist threats that could occur within its area of responsibility and gathers, analyzes, and disseminates information which would assist the relevant responsible agencies (e.g., law enforcement, intelligence, and critical infrastructure) with the prevention, protection, response, or recovery efforts of those incidents.

Critical Infrastructure—Assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, public health or safety, or any combination thereof.

Critical Infrastructure Protection Activities—These activities may include (1) efforts to understand and share information about terrorist threats and other hazards as related to critical infrastructure, (2) building security partnerships, (3) implementing a long-term risk management program, and (4) maximizing the efficient use of resources related to critical infrastructure protection. Examples include, but are not limited to (1) providing critical infrastructure owners and operators with timely, analytical, accurate, and useful information on threats to critical infrastructure; (2) ensuring that industry is engaged as early as possible in the development and enhancement of risk management activities, approaches, and actions; and (3) developing resources to engage in cross-sector interdependency studies through exercises, symposiums, training sessions, and computer modeling.

-D-

DEA Internet Connectivity Endeavor (DICE)—A system for queries from any law enforcement agency, intended to provide national deconfliction of investigation activity.

Disclaimer—Any statement intended to specify or delimit the scope of rights and obligations that may be exercised and enforced by parties in a legally recognized relationship.

Dissemination Matrix—A document used by fusion center personnel to ensure the proper review, handling, and dissemination of products. Typically, a dissemination matrix identifies fusion center customers, classification, and handling caveats; details peer and supervisory reviews; and identifies the dissemination method for each fusion center product type.

Documented Plan, Policy, or SOP—A written or typed plan, policy, or SOP defined in document form.

Draft—Description of a document that has not yet been approved by a fusion center's required approval authority (e.g., fusion center governance body, Homeland Security Advisor, Fusion Center Director).

-E-

Emergency Operations Center (EOC)—The physical location where the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., federal, state, regional, tribal, city, county), or some combination thereof.

Exercise—The employment of personnel and resources in a controlled environment to test, validate, and/or improve a specific plan or capability in pursuit of a stated objective. Exercises may include workshops, facilitated policy discussions, seminars, tabletop exercises, games, modeling and simulation, drills, functional exercises, and full-scale exercises.

-F-

Fair Information Practice Principles—A general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. Different organizations and countries have their own terms for these standards. The U.S. Department of Homeland Security (DHS) has identified a set of eight principles, rooted in the tenets of the Privacy Act of 1974, that account for the nature and purpose of the information being collected in relation to an organization's mission.

Federal Bureau of Investigation Network (FBINet)—A classified network run by the FBI that facilitates information sharing for fusion centers.

Federal Resource Allocation Criteria Policy—A federal policy (Information Sharing Environment Guidance ISE-G-112) that defines objective criteria to be used by federal departments and agencies when making resource allocation decisions to fusion centers.

Federal Share—The share or amount of a fusion center cost that is paid for by an agency within the federal government (including grants).

Federally Declared Disaster—A major disaster can be a result of a hurricane, an earthquake, a flood, a tornado, or a major fire; the President then determines whether the situation warrants supplemental federal aid. The event must be clearly more than state or local governments can handle alone. If a major disaster is declared, funding comes from the President's Disaster Relief Fund, managed by FEMA, and disaster aid programs of other participating federal agencies. A Presidential Major Disaster Declaration puts into motion long-term federal recovery programs, some of which are matched by state programs and designed to help disaster victims, businesses, and public entities.

Financial Audit—Verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is a reasonable assurance that the financial statements are presented fairly, in all material respects, or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to enhance the degree of confidence of intended users in the financial statements. No element of the annual Assessment process (including the Cost Assessment) is intended to serve the purpose of a financial audit.

Financial Crimes Enforcement Network (FinCEN) Project Gateway—Affords law enforcement officials in each state online access to financial crime databases at FinCEN, a U.S. Department of the Treasury bureau under the Treasury Under Secretary for Terrorism and Financial Intelligence.

Formal—Following or in accordance with an established form, custom, or rule (e.g., formal training is training that follows a specified format, such as activities designed to achieve targeted results versus informal training that might occur spontaneously and/or casually).

Fusion Center Customers—Users, consumers, or recipients of fusion center analysis, information, or intelligence products. Customers can be individuals or organizations.

Fusion Liaison Officer (FLO)—Individuals who serve as the conduit for the flow of homeland security and crime-related information between the field and the fusion center for assessment and analysis. FLOs can be from a wide variety of disciplines, provide the fusion center with subject matter expertise, and may support awareness and training efforts. Fusion centers may use various names for FLOs, such as Terrorism Liaison Officer, Intelligence Liaison Officer, and Field Intelligence Officer.

FLO Program—FLO programs vary in focus, complexity, and size, but all have the same basic goal of facilitating the exchange of information between fusion centers and stakeholders within the fusion center's area of responsibility.

Fusion Process—The overarching process of managing the flow of information and intelligence across levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. The fusion process turns information and intelligence into actionable knowledge.

-G-

Governance Body—An oversight entity composed of officials with decision-making authority, capable of committing resources and personnel to a fusion center.

-H-

High Intensity Drug Trafficking Areas (HIDTA)—A program created by Congress with the Anti-Drug Abuse Act of 1988 that provides assistance to federal, state, local, and tribal law enforcement agencies operating in areas determined to be critical drug trafficking regions of the United States.

Homeland Secure Data Network (HSDN)—Secret-level information network intended to provide Secret-level information sharing capability to fusion centers and other partners.

Homeland Security Grant Program (HSGP)—Composed of three interconnected grant programs—State Homeland Security Program (SHSP), Urban Areas Security Initiative (UASI), and Operation Stonegarden (OPSG)—that fund a range of preparedness activities, including planning, organization, equipment purchase, training, exercises, and management and administration.

Homeland Security Information Network (HSIN)—A U.S. Department of Homeland Security-managed national secure and trusted Web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

Homeland Security Information Network Intelligence Community of Interest (HSIN Intel)—A subset of HSIN for state and local intelligence. It is a U.S. Department of Homeland Security-owned and -operated, user-driven, Web-based, unclassified sharing platform connecting homeland security mission partners.

Homeland Security Standing Information Needs (HSEC SINs)—Refers to the enduring all-threats and all-hazards information needs of the U.S. Department of Homeland Security and its federal, state, local, tribal, territorial, and private sector stakeholders and homeland security partners.

-|-

“If You See Something, Say Something™” Campaign—A U.S. Department of Homeland Security program to raise public awareness of indicators of terrorism and violent crime and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities.

Implement—To put into effect (i.e., to implement a plan by communicating it to internal and/or external stakeholders, training staff on it, and incorporating it into a fusion center’s day-to-day activities).

Incident—An occurrence, natural or man-made, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

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 Needs—The data and information needed by intelligence analysts in order to answer intelligence questions; types of information the intelligence unit needs and intends to gather from all available sources through passive and active collection and/or reporting.

Information Sharing Environment (ISE) Privacy Guidelines—Principles for federal departments and agencies to follow to ensure that the information privacy rights and other legal rights of Americans are protected as personally identifiable terrorism-related information is acquired, accessed, used, and stored in the ISE.

InfraGard—A partnership between the FBI and businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard chapters are geographically linked with FBI Field Office territories.

In-Kind Resource—A noncash input provided to a fusion center that can be given a cash value (e.g., services of a detailee from another agency).

Integrated Border Enforcement Teams (IBETs)—Joint units composed of U.S. and Canadian law enforcement agencies whose mission is to enhance border integrity and security along the shared Canada/United States border—between designated ports of entry—by identifying, investigating, and interdicting persons, organizations, and goods that threaten the national security of one or both countries or that are involved in organized criminal activity.

Intelligence—Actionable inference or a set of related inferences derived from some form of inductive or deductive logic. By combining information, analysis, and interpretation, intelligence helps to document a threat, ascertain its probability of occurring, and define a responsive course of action, all in a timely manner.

Interdependencies—Multiple dependencies between two or more infrastructures.

Investigative Personnel—Fusion center personnel who primarily conduct investigations related to potential criminal or terrorist acts that have occurred and/or that may occur, such as individuals from the fusion center assigned to the Joint Terrorism Task Force.

Issue-Specific Training—Training provided to fusion center analysts on issues (such as risk analysis, finance, critical infrastructure protection, counternarcotics, or gangs) that are consistent with the center's mission and analysts' roles and responsibilities.

-J-

Joint Terrorism Task Forces (JTTFs)—Multijurisdictional task forces established to conduct terrorism-related investigations. JTTFs focus primarily on terrorism-related issues, with specific regard to terrorism investigations with local, regional, national, and international implications.

Joint Worldwide Intelligence Communications System (JWICS)—A 24-hour-a-day network designed to meet the requirements for secure (TS/SCI) multimedia intelligence communications worldwide.

-L-

Law Enforcement Online (LEO)—A virtual private network accredited and approved by the FBI for sensitive but unclassified information. Used by all levels of the law enforcement, criminal justice, and public safety communities to support investigative operations, send notifications and alerts, and provide an avenue to remotely access other law enforcement and intelligence systems and resources.

Legal Personnel—Fusion center personnel who provide legal guidance and/or oversight concerning fusion center activities. These personnel typically have law degrees and provide guidance and oversight for fusion center activities regarding privacy, civil rights, and civil liberties and other legal issues and protections.

Liaison/SME Personnel—Fusion center personnel who do not work primarily as analysts in the fusion center but who are subject matter experts (SMEs) in a discipline relevant to the fusion center (e.g., critical infrastructure, emergency management) and/or serve as liaisons to partner agencies or organizations of the fusion center.

Local Context—The set of conditions or the environment associated with a geographic area or jurisdiction. A fusion center can apply a local context to any analysis it does that would involve considering local issues, conditions, implications, and other locally generated information. When considering federally generated information or other information received from outside of the local area, applying a local context would involve any additional analysis that would make that information more relevant, relatable, or actionable to stakeholders within a particular jurisdiction.

For example, with national threat information, it could mean conducting analysis to determine potential impacts to a particular jurisdiction.

-M-

Management/Administrative Personnel—Fusion center personnel who primarily provide executive management of the fusion center (e.g., Fusion Center Director, Deputy Director) or primarily aid executive management by coordinating such office services and procedures as the security, supervision, maintenance, and control of the flow of work and programs, personnel, budgeting, records, etc., for the fusion center. Also includes fusion center personnel who provide administrative support (e.g., office managers, budget and grant analysts).

Maritime Interagency Operations Center (IOCs)—Maritime IOCs are intended to share maritime information by better planning, coordinating, and executing operations with the U.S. Coast Guard's port partners (other agencies and organizations with which it coordinates).

-N-

National-Level Risk Assessment—Product or process that collects information on issues of significant national concern and assigns values to risks for the purpose of informing national priorities, developing or comparing courses of action, and informing decision making.

National Special Security Event (NSSE)—An event of national significance designated by the Secretary of Homeland Security that, by virtue of its political, economic, social, or religious significance, may be a target of terrorism or other criminal activity. Events include presidential inaugurations, major international summits held in the United States, major sporting events, and presidential nominating conventions.

National Terrorism Advisory System (NTAS)—NTAS replaces the color-coded Homeland Security Advisory System. Its purpose is to effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

National Virtual Pointer System (NVPS)—A U.S. Department of Justice system that provides federal, state, local, and tribal law enforcement agencies with access to pointer databases through a single point of entry to determine whether any other law enforcement entity is focused on the same investigative target.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—A unified process for reporting, tracking, and accessing SAR in a manner that rigorously protects the privacy and civil liberties of Americans.

NSI Analyst Training—An eight-hour workshop-format training focused on ensuring that SARs are properly reviewed and vetted to promote the integrity of information submitted; protect citizens' privacy, civil rights, and civil liberties; and successfully implement the SAR process.

NSI Compliance—Deemed by the NSI to be compliant with NSI requirements.

Neighborhood Watch Programs—Local crime prevention programs initiated either by the public or the police that involve citizens in crime prevention activities.

-P-

P/CRCL Outreach Plan—A plan for the engagement of a fusion center with internal and external stakeholders to promote the fusion center's privacy, civil rights, and civil liberties protections, processes, and efforts.

Primary Fusion Center—In each of the 50 states, the District of Columbia, and the five territories, a fusion center that is designated by the Governor as the primary fusion center, pursuant to the joint U.S. Department of Homeland Security and U.S. Department of Justice November 2007 fusion center designation letter and in accordance with the Federal Resource Allocation Criteria policy.

Private Sector—Includes business (both profit and nonprofit), commerce, associations, academia, and industry.

Public Affairs Officer/Public Information Officer—An individual designated by an appointing official or entity who is responsible for the initiation, development, production, and implementation of public relations and public communications plans, materials, and strategies.

-R-

Real-Time Crime Center (RTCC)—Also referred to as Crime Analysis Centers (CACs), RTCCs are analytic-driven centers located in law enforcement agencies that utilize technological and analytical capabilities to provide real-time information to officers responding to service calls and developing situations.

Recognized Fusion Center—A fusion center that has been designated as a fusion center by the Governor of the state but that has not been designated as the state's primary fusion center, in accordance with the Federal Resource Allocation Criteria policy.

Regional Information Sharing Systems® (RISS) Centers—Funded through grants administered by DOJ's Bureau of Justice Assistance (BJA), RISS Centers support regional law enforcement, public safety, and homeland security efforts to, among other things, combat major crimes and terrorist activity and promote officer safety by linking federal, state, local, and tribal criminal justice agencies through secure communications and providing information sharing resources and analytical and investigative support.

Regional Information Sharing Systems® Network (RISSNET™)—Managed by the Regional Information Sharing Systems (RISS) and now known as the RISS Secure Cloud, RISSNET is a secure national intranet to facilitate law enforcement communications and information sharing nationwide.

Representatives—Personnel funded by a partner agency.

Request for Information—A request initiated by the fusion center or a fusion center stakeholder (e.g., law enforcement agency or the U.S. Department of Homeland Security) that could include, but is not limited to, requests for information or intelligence products or services such as name traces, database checks, assessments, subject matter expertise assistance, or finished intelligence products.

Risk—The potential for an unwanted outcome resulting from an incident, an event, or an occurrence, as determined by its likelihood and the associated consequences.

Risk Assessment—A product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

-S-

Secure Internet Protocol Router Network (SIPRNet)—SIPRNet is the U.S. Department of Defense network for the exchange of classified information and messages at the Secret level.

Security Liaison—An individual designated by an appointing official or entity who is responsible for ensuring the security of the fusion center, including personnel, information, equipment, and facilities.

Sensitive Compartmental Information Operational Network (SCION)—The FBI enterprise network for processing, transmitting, and storing information at the Top Secret/Sensitive Compartmented Information level.

Situational Awareness Products—A situational awareness product describes an event or incident of interest to customers (e.g., BOLOs, notes, event reports, daily bulletins, SITREPs, raw reporting).

Sovereign Citizen Extremists—Groups or individuals who facilitate or engage in acts of violence directed at public officials, financial institutions, and government facilities in support of their belief that the legitimacy of the US citizenship should be rejected; almost all forms of established government, authority, and institutions are illegitimate; and that they are immune from federal, state and local laws.

Special Event Assessment Rating (SEAR)—SEAR events are those preplanned special events below the level of National Special Security Events that have been submitted via the annual National Special Event Data Call. The majority of these events are state and local events that may require support augmentation from the federal government.

Standing Information Needs (SINs)—Enduring information needs about the homeland security threat or operational environment. SINs provide a formal, structured framework for categorizing issues and topics of interest for fusion centers.

Statewide Fusion Center Coordination Plan—Identifies the roles, responsibilities, and coordination efforts for each fusion center within a state in carrying out the fusion process within that state.

Strategic Analysis—Strategic analytic products included assessments providing an overall picture of the intent and capabilities of specific terrorist or criminal groups, including likely tactics, techniques, and procedures. Strategic analytic products might also include trend analysis and forecasting.

Strategic Plan—A plan that defines an organization's or an entity's vision, mission, goals, and objectives, identifying the strategic programmatic and operational priorities for a discrete period of time.

Subject Matter Expert—A person who is an expert in a particular area or topic.

Suspicious Activity Reporting (SAR)—Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

-T-

Tactical Analysis—Tactical analytic products assess specific, potential threats related to near-term timeframes or major events. They involve issues that need immediate information capabilities to assist decision making on current operations. Tactical cyber analysis includes analysis of cyber indicators, to include but not limited to Internet Protocol addresses, domains, hashes, and log files, for the purpose of assisting in case support or operational goals.

Tag—To mark or provide with an identifying marker (e.g., to mark products with the Standing Information Needs they address).

Targeted Violence Information Sharing System (TAVISS)—U.S. Secret Service centralized database of names of subjects, allowing name checks to determine whether an individual is of protective interest to any other agency within the TAVISS network.

Threat—Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Threat and Hazard Identification and Risk Assessment (THIRA)—A four-step common risk assessment process that helps the whole community—including individuals, businesses, faith-based organizations, nonprofit groups, schools and academia, and all levels of government—understand its risks and estimate capability requirements. See FEMA's *Comprehensive Planning Guide 201: Threat and Hazard Identification and Risk Assessment*, Second Edition, for additional information.

Threat Assessment—An assessment of a criminal or terrorist presence within a jurisdiction combined with an evaluation of the 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.

Tips and Leads—Information provided from fusion center stakeholders, the general public, or other sources regarding potentially criminal or illicit activity, but not necessarily or obviously related to terrorism.

Training/Exercise Personnel—Fusion center personnel whose primary role is the development or delivery of mandatory or mission-relevant elective training and/or the development of, planning for, or execution of exercises.

-V-

Vulnerability—Physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.

Vulnerability Analysis or Assessment—An analysis 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.