



FOR OFFICIAL USE ONLY



**TERRORIST THREATS  
TO THE US HOMELAND (U)**  
REPORTING GUIDE



FOR OFFICIAL USE ONLY

**Terrorist Threats to the U.S. Homeland Reporting Guide**

**Note**

This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS and FBI policy relating to FOUO information and is not to be released other than to law enforcement and homeland security personnel, without prior approval of an authorized DHS or FBI official.

**Information in this document is NOT for general public dissemination and must remain under government control. Its dissemination should be limited to official government use and is not authorized for electronic dissemination or transfer to nongovernmental channels or media.**

May contain copyrighted materials. Reproduction or further dissemination of this work is prohibited without the permission of the copyright holder.

**This Reporting Guide is intended to complement the reader's knowledge of possible indicators of terrorist activity. It does not establish independent authority to conduct intelligence gathering activities, nor is it an intelligence collection tasking or request. Recipients are encouraged to consult with their legal counsel as to any questions regarding the scope of their legal authorities.**

## Table of Contents

<b>Note.....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b><i>Introduction.....</i></b>	<b>3</b>
<b><i>Reporting Guidance .....</i></b>	<b>4</b>
<b>Personnel, Organization, and Areas of Activity.....</b>	<b>5</b>
Leaders.....	5
Members/Operatives/Supporters.....	5
Organizational Structure .....	12
Areas of Activity.....	12
<b>Capabilities .....</b>	<b>14</b>
Readiness .....	14
Acquisition of Expertise .....	16
Material.....	18
Intelligence/Security .....	22
Logistics/Infrastructure.....	25
<b>Operations (Terrorist Attacks).....</b>	<b>32</b>
Objectives of Attack .....	32
Type of Attack .....	33
Plans/Tactics .....	35
Targeting.....	36
Timing/Sequencing.....	38
Operational Reconnaissance or Surveillance.....	39
Operational Security .....	40
Movement to/from Target; Staging .....	42
<b>Criminal Activities (Non-Operations).....</b>	<b>44</b>
Inside the Continental United States.....	44
Outside the Continental United States .....	44
Nature/Purpose of Illegal Acts .....	44

*Introduction*

This **Terrorist Threats to the U.S. Homeland Reporting Guide** (TTRG) was jointly produced by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS). The purpose of this document is to leverage the vast information collection and reporting resources of our state, local and tribal law enforcement partners, as well as other first responder partners, in recognizing activities or conditions that may be indicative of terrorist activity. State and local organizations are on the front line in the war against terror and therefore have a critical role as primary sources of information. Timely and relevant information from the “front lines” is critical to the identification of terrorists and their supporters, development of insights into their plans and intentions, and subsequent disruption of their operations.

Al-Qaida and its affiliated elements within the Sunni extremist movement pose the greatest terrorist threat to the U.S. Homeland. The number of individuals and groups who subscribe to the al-Qaida philosophy, the breadth of their recruitment base, their ability to operate clandestinely on a global scale, their strong anti-American sentiment, and their demonstrated willingness to inflict large numbers of casualties portend a persistent threat, notwithstanding significant counterterrorist successes.

This guide can be found on Law Enforcement On-line (LEO) at <http://www.leo.gov> and by clicking on the TTRG tab on the following Homeland Security Information Network (HSIN) / Joint Regional Information Exchange System (JRIES) portals:

- Law Enforcement (LE): <https://jries.dhs.gov>
- Combating Terrorism (CT): <https://ct.jries.dhs.gov>
- Emergency Operations Center (EOC): <https://eoc.jries.dhs.gov>

Intelligence produced as a result of the use of this guide will be routinely published on LEO and disseminated through other DHS and FBI channels.

*Reporting Guidance*

DHS and FBI encourage recipients of this Reporting Guide to report information concerning suspicious or criminal activity potentially related to terrorism initially to their local FBI Joint Terrorism Task Force (JTTF) – the FBI regional phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm> – and subsequently to the Homeland Security Operations Center (HSOC) via telephone at 202-282-8101 or by email at [TTRG.reporting@dhs.gov](mailto:TTRG.reporting@dhs.gov).

Each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting organization and a designated point of contact (POC). To facilitate reporting to the HSOC, DHS has created a web-based reporting form accessible via the TTRG tab on the HSIN/JRIES portals.

The FBI has compiled the following list to assist law enforcement agencies at all levels in recognizing and reporting potential terrorist activities. The information is organized into four general areas:

- Personnel, Organization, and Areas of Activity
- Capabilities
- Operations
- Criminal Activities (non-operational)

## **Personnel, Organization, and Areas of Activity**

### **Leaders**

#### **Identities, descriptions, and backgrounds of terrorist leaders and key operatives in the United States and abroad**

Indicators/Reportable Items:

- Many individuals in contact with the same person for guidance, to obtain funds, facilitate fund raising, recruitment, criminal activities, etc.
- Communication to/from the same locations using coded references to leadership, key figures or key functions (e.g., bomb maker)
- Attendance at meetings of key leaders, planners or operatives
- Participation in/control of the decision making process
- Individual has access to a known leader

### **Members/Operatives/Supporters**

#### **Identities, descriptions, and backgrounds of terrorist members/operatives, supporters and collaborators**

Indicators/Reportable Items:

- Physical descriptions, photographs, aliases, Internet identities, locations, background, education, ideology, citizenship, date-of-birth, and nationality
- Illnesses or health problems; use of alcohol, tobacco, or drugs/medications
- Hobbies, habits, personality and behavioral traits
- Biometric information such as fingerprints and DNA samples
- Employment and/or sources of income
- Religious background by birth or conversion
- Tribe, clan and familial ties
- Professional associations and affiliations
- Passport or visa numbers
- Languages spoken
- Criminal record
- Travel plans and history
- Information related to U.S.-based individual appears in terrorist's email buddy list, email message, address book (paper or electronic), pocket litter, or other type of contact list

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Mention of U.S.-based individual by known or suspected terrorist(s)
- Individual appears in photographs with known terrorist suspects
- Specialized journal/magazine subscriptions
- Individual originates from a country of concern and provides inaccurate/incomplete travel information
- Travel to areas known to harbor terrorists or to serve as support bases
- Possession of documents that appear to have been doctored or do not conform to official standards
- Attendance at closed or secret meetings
- Associations with known or suspected terrorists and/or terrorist front organizations
- Affiliation with individuals who are known or suspected extremist supporters or sympathizers
- Participation in violent political, religious, terrorist, or insurgent/guerrilla actions
- Associations with clerics or institutions known to have affiliations with radical movements and state sponsors
- Relations with extremist religious, nationalist, ethnic separatist, or anti-globalization groups
- Communications between individuals in the United States and known or suspected extremists in safe havens abroad
- Attendance at venues known to preach or to be associated with radical/anti-U.S. views
- Jihadist literature, terrorist training manuals, security plans, encoded materials, or instructions for the use of codes and ciphers in residence or vehicle
- Activities in the United States do not match the stated purpose of visa
- Suspicious travel-related documentation or “pocket litter” containing information on U.S. or foreign contacts
- Group composed largely of individuals whose absence from jobs or families would not attract attention (e.g., young, single males with no professional ties) and who are unknown to law enforcement or intelligence services
- Discussion of, or a movement towards, violence by newly coalescing groups or previously known political or dissident groups
- Use of the Internet by affiliated individuals using racist, alarmist, or extremist rhetoric
- Policy statements or commentary advocating violence
- Affiliations with organizations involved in supporting, advocating or implementing violent acts
- Sponsorship of visas for individuals with known or suspected ties to terrorism
- Arranged marriages to facilitate U.S. citizenship

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Presence in a residence of weapons such as knives, pistols, rifles, rocket launchers, explosives, poisons, or precursor materials, or receipts for same
- Evidence of inquiries to companies involved in the production or distribution of weapons such as knives, pistols, rifles, rocket launchers, explosives, poisons, or precursor materials
- Cache(s) of funds, some of which may be held by unwitting associates
- Cache(s) of personal identification documents stored in other than the usual locations (e.g., desks, dressers, closets) or containers (e.g., lock boxes or plastic storage containers), including on computers
- Possession of identification documents bearing more than one identity
- Possession of passport photos of other individuals
- Indirect communications, such as the use of cutouts or a series of meetings in succession
- Inability to provide personal background information beyond that contained in documents carried on-person or a seemingly practiced set of facts
- Invalid or unusual explanations of visitor, employment, or student status
- Significant differences in a subject's appearance and photos in identity documents (e.g., individual without a beard, even though the individual is known to follow religious convention)
- No record of travel to the country in which the individual holds a valid passport
- Exclusive use of public telephones and/or telephone cards by individuals who otherwise have an address or residence
- Use of coded or general terms while speaking on the telephone
- Conducting periodic examinations of the telephone wire and receiver
- Presence of coded telephone numbers disguised as prices for shopping lists or item serial numbers
- Use of authentication techniques to confirm the identify of the called party
- Altering the voice when discussing sensitive subjects
- Sudden discontinued use of a telephone number, email account, or other means of communication (on the assumption its use is no longer secure)
- Postmarking letters at a distant post office rather than a local one
- Personal letters received from abroad addressed to P.O. boxes or to individuals or locations other than the individual's place of residence
- Individual appears in a video associated with a specific terrorist group or speaks out on behalf of / promotes a terrorist organization
- Variations in arrival and departure times to and from the subject's residence and variations in the routes used to and from the residence
- Individual is former Mujahidin with suspected ties to terrorists
- Use of intermediaries to obtain identification cards or documents



## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Tests of security at airports, railway terminals, or border crossings
- Individual brags of association with known or suspected terrorists
- Individual seeks out or possesses information on critical infrastructure (e.g., visits websites about dams or water supply, possesses a marked-up almanac, etc.)
- Contacts with smugglers or organized crime
- Individual is in possession of blueprints, maps, or photographs of sensitive locations and potential targets
- Individual's residence contains little or no furniture besides a bed or mattress, a table and chair, etc.
- Individual's residence contains police manuals, military training manuals, flight manuals, first-responder radio scanners or other communications equipment, surveillance equipment such as night-vision goggles, GPS devices, or still and video cameras
- Presence of computers, scanners, and laminators that may indicate that identification documents are being made

### **Methods that may be used to recruit terrorist members/supporters in the United States**

Indicators/Reportable Items:

- Frequent contact with disaffected populations (e.g., prisoners, radical student groups, members of radical mosques)
- Frequent contact with family members sympathetic to radical movements or violent social action
- Unique or novel methods such as youth camps, Internet blogs or virtual communities
- Offer or provision of paramilitary training

### **Types of individuals that may be targeted for recruitment in the United States, and their qualifications**

Indicators/Reportable Items:

- Presence of recruiters or recruiting materials at target pools, including schools, cultural centers, youth camps, prisons, military, and in populations sympathetic to the terrorist cause
- Presence of recruitment material on Internet sites or recruitment discussions in chat rooms
- Recruitment efforts targeting individuals with special interest professions (food sciences, husbandry, microbiology, toxicology, pharmaceuticals), cultural, religious, special interest groups or individuals associated with federal research programs
- Attempts to recruit individuals who are "Western" in appearance

**Possible assessment factors used by terrorists to select recruits**

Indicators/Reportable Items:

- Source statements, documents, publications or any other media that describes desirable characteristics for potential recruits, or alternatively, characteristics that would warrant rejection or marginalization of potential candidates
- Test of individual's willingness to perform specified task, travel or endure hardship
- Test of individual's ability to procure materials
- Test of an individual's willingness to accept religious indoctrination
- Recruits who are "Western" in appearance who might be less likely to be scrutinized by security personnel

**Entities that may be actively working with terrorist groups**

Indicators/Reportable Items:

- Providing material support (e.g., funding, arms, safe havens, false documents, personnel support) to terrorists by a foreign entity
- Relations with states where terrorists are believed to be located and protected
- Identities and descriptions of non-traditional cover agents in the United States affiliated with state sponsors of terrorism
- Attendance at events sponsored by governments known to support terror
- Frequent travel by staff members or leaders to terrorist safe havens or territory controlled by state sponsors
- Non-governmental organization (NGO) staff composed of individuals with ties to or membership in terrorist-related organizations
- Granting of special favors to suspect individuals or groups by a foreign entity or NGO (e.g., monetary grants, debt relief, training, status, bona fides)
- Contacts with foreign intelligence and security services or affiliates for the purpose of information sharing, training, financing and logistical support
- Material support to individuals or groups affiliated with anti-U.S. terrorist activities
- Communications/contacts between members of established groups or state sponsors and splinter/surrogate groups
- Direct or indirect contacts or affiliations between terrorists and NGOs
- Suspicious financial transactions involving NGOs who arrange travel for staff, consultants, aid workers or students
- Frequent foreign travel to area(s) of concern

- Frequent opening and closing of businesses in the United States

**Role of U.S.-based members/supporters in overall terrorist group activities/operations**

Indicators/Reportable Items:

- Evidence of surveillance activities at potential targets
- Maps, almanacs, and information possibly highlighting potential targets found in the possession, residence or on the computer of a terrorist suspect
- Suspect's residence being used to house overseas guests
- Suspect sponsoring foreign national from country of interest for purposes of entry into the United States
- Conducting illegal operations to facilitate operations (cigarette smuggling for financial gain, bribery for passports and documentation, harboring illegal aliens)
- Providing legal education materials that describe how to evade U.S. laws or screening procedures
- Friendships being forged with individuals who are in a position to, or have specialized skills that would, assist the operations of the group (e.g., police, government employees)
- Suspects infiltrating ethnic communities to recruit for the cause
- U.S. based members sharing advice on how foreign operatives should behave while in the United States to avoid detection
- Identification of significant U.S. holidays/events that could indicate timing/venue for attack
- Efforts by operatives to infiltrate existing Muslim communities
- Efforts by operatives to solicit funding from mosques or local community members
- Efforts by operatives to infiltrate Islamic charities

**Indications that leaders of terrorist groups abroad may be in contact with individuals in the United States**

Indicators/Reportable Items:

- Phone contact between foreign and domestic terrorist suspects
- Internet contact between foreign and domestic terrorist suspects
- Wire transfers between foreign and domestic terrorist suspects
- Business dealings between foreign and domestic terrorist suspects
- Meetings between foreign and domestic terrorist suspects
- Transfer of money, weapons or operational materials between foreign and domestic suspects

**Possible use of surrogate, splinter or infiltrated groups to attack U.S. interests**

Indicators/Reportable Items:

- Statements or documentation suggesting a formal or informal alliance has been reached between groups that were not previously known to cooperate
- Discussion of surrogate, splinter or infiltrated groups by known or suspected terrorists
- Expressions of sympathy for known or suspected terrorists expressed by individuals associated with surrogate, splinter or infiltrated groups

**Types of support that terrorist groups might be providing to one another**

Indicators/Reportable Items:

- Evidence of inter-group assistance with logistics, training and meeting facilities, smuggling services, assistance with infiltration of operatives, provision of travel services, related identification documentation, and/or recruiting efforts
- Evidence of inter-group assistance or cooperation in training, surveillance, reconnaissance, diversionary or direct-fire support and/or attacks
- Evidence of inter-group sheltering or maintenance of assets or financial instruments, cooperation in illicit activities for profit, or other financial activities for mutual benefit
- Common training facility or instructor(s) used by different terrorist groups
- Contact between member(s) or leader(s) of two or more terrorist groups
- Common logistical support used by different terrorist groups (e.g., travel facilitator)

**Indications that organized crime, drug-trafficking organizations or other criminal enterprises may be actively supporting terrorist groups**

Indicators/Reportable Items:

- Evidence of enterprise/syndicate-group assistance with logistics such as smuggling services, assistance with infiltration of operatives, provision of travel services and/or related identification documentation

**Patterns of activity that may be evident when a new cell is forming**

Indicators/Reportable Items:

- Coalescence of various loosely affiliated individuals/groups

**Organizational Structure**

**How a terrorist group is organized (e.g., hierarchical, network, decentralized, autonomous cells)**

Indicators/Reportable Items:

- Coalescence of various loosely affiliated individuals into a cell-like structure
- Individual has pattern of contact (e.g., receives a call from A and immediately calls B)

**Command-and-control structure, to include roles, functions, lines of authority and decision-making process**

Indicators/Reportable Items:

- Decision-making and operational planning processes
- Functional responsibilities within a terrorist organization
- Qualities/path for advancement
- Path of succession
- Cliques/conflicts within an organization

**Areas of Activity**

**Where terrorist groups may be active (e.g., fund raising, recruiting, training, meeting) within the United States**

Indicators/Reportable Items:

- Identified nodes, clusters or groupings of locations associated with terrorist support activities
- Travel of multiple individuals converges on location

**Where terrorist key facilities (e.g. training site, weapons stores, safe houses) are located**

Indicators/Reportable Items:


- Co-location of command and control elements
- Selection of storage areas with heat and humidity controls or protection
- Selection of semi-secluded areas with access to parks or other public places
- Frequent or sudden turnover in tenants of a dwelling
- Use of rooms that are seldom used by occupants or family members
- Use of an observation vehicle to provide early warning while en route to or from the cache site
- Use of surveillance detection techniques en route to or from the cache site
- Infrequent visits by the individual responsible for the storage area
- Presence of rental or other covered or refrigerated vehicles at storage facilities
- Spikes or large increases in utility usage, i.e., much larger than normal electric or water bills
- Evidence of a laboratory being moved in response to detection with few materials abandoned

## Capabilities

### Readiness

#### **Types of attack (Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) and non-lethal) that terrorist groups are capable of executing**

Indicators/Reportable Items:

- Evidence of production of precursor chemicals and agents, including advanced nerve agents, infectious bacterial and viral agents, and toxins
- Evidence of vaccinated personnel or personnel on antibiotic treatment
- Purchase of equipment and access to laboratories to develop chemical or biological toxins or agents
- Acquisition of biological cultures or microorganisms, vaccines and preventative medicines, chemicals, nuclear or radiological material, protective gear, special or unique technical or laboratory equipment, small animals, or dual use items
- Acquisition of equipment, components and related materials for the design and/or fabrication of nuclear/radiological devices by organizations or individuals with extremist connections or sympathies
- Ties to research labs, medical facilities, or companies able to purchase CBRNE-type materiel, equipment, or suspicious or dual-use items
- Evidence of pharmaceutical or agricultural production facilities with apparent change in production mission
- Attempts to gain access to farming equipment including seed planes that could be used to spread toxic substances
- Attempts to obtain crop toxins or insects that could poison or severely damage the food supply
- Interest in acquisition or culturing of livestock disease pathogens
- Sudden illness of livestock herds or human population in a local area
- Modification of truck or van with heavy duty springs to handle heavier loads
- Test explosions in remote areas
- Treatment of or presence of untreated chemical burns or missing hands/fingers
- Individuals inquire or attempt to secure antidotes to poisons not found in a normal course of activity, including antibiotics
- Treatment of unusual disease(s)
- Evidence of inquiries to companies involved in the production or distribution of possible precursors (listed in the next section)
- Evidence of procurement of precursors (listed in the next section)
- Evidence of storage of precursors (e.g., storage facility)
- Evidence of use of small animals for testing purposes 

**Readiness levels (quality and sufficiency) of terrorist group manpower, training, weapons and positioning**

Indicators/Reportable Items:

- Evidence of completed assembly of device
- Rental of chemical sprayers, spraying vehicles or aircraft
- Sudden illness of livestock herds or human population in a local area
- Willingness to use untrained individual in a CBRNE attack
- Individual purchases of paint or decals similar to those found on local office or food supply delivery vehicles and/or emergency response vehicles, or the theft of same
- Theft or purchasing attempts of security, first responder or maintenance services uniforms, access badges or related equipment
- Attempted acquisition of any of the following precursor chemicals:

*(specified amounts represent minimum required to produce a significant attack):*

Nerve or Blood Agent Precursors:

- Diethylamine (18-liter qty.)
- 2-ethanethiol HCl (100-gram qty.)
- 2-(diethylamino) ethanol (18-liter qty.)
- Diisopropylamine (1-liter qty.)
- 2-diisopropylamino ethanol (500-ml qty.)
- Methyl phosphonyl dichloride (25-gram qty.)
- Phosphorous oxychloride (1-liter qty.)
- Phosphorous pentachloride (5- kg qty.)
- Phosphorous pentasulfide (1-kg qty.)
- Phosphorous trichloride (1-liter qty.)
- Pinacolone (500-ml qty.)
- Pinacolyl alcohol (100-gram qty.)
- Thiodiglycol (500 gram qty.)

Hydrogen Cyanide Precursors:

- Sodium cyanide (6 kg qty.)
- Sulfuric acid (15-liter qty.)

Mustard Agents:

- Benzene (20-liter qty.)
- Isopropanol (20-liter qty.)
- Sodium fluoride powder (12 kg qty.)
- Methyl phosphonyl dichloride (25-gram qty.)
- Thiodiglycol (500 gram qty.)
- Hydrochloric acid (15-liter qty.)
- Hydrogen chloride gas (130 kg qty.)



## Acquisition of Expertise

### Types of training that terrorist group members or supporters are receiving, where and from whom

Indicators/Reportable Items:

- Attempts to obtain or conduct organized training in security concepts, conventional military weapons and tactics and CBRNE weapons
- Website details “how to” instructions for terrorist activities
- Conduct of military-type training located at a distance from populated areas
- Training location secluded but accessible from a number of roads and entrances, and may or may not be equipped with living quarters
- Training location known only by those serving as trainers and trainees
- Use of guards, lookouts or other security measures during training
- Exclusion of anyone not connected with the training
- Concealment of training activity and equipment after training
- Conduct of training by small groups
- Trainers and trainees do not know each other’s identities
- Specialized training such as explosives, firearms, survival, flight school or defensive driving
- Obtain copies of dissertations/theses espousing radical views, or address technological issues of interest to terrorists
- Training in surveillance, weapons, or in intelligence-gathering techniques
- Training sponsored by known or suspected terrorists
- Reports of explosions, gunfire, or unexplained fires in remote, rural or vacant industrial areas
- Individuals displaying burns or chemical exposure symptoms with vague or irrational explanations as to the circumstances surrounding the injuries
- Suspicious surveillance incidents or suspicious activities near potentially targeted facilities that are associated with the same two or three individuals
- Abandoned, disabled delivery vehicles discovered with no registration information and/or missing VIN
- Rescues made from burning buildings or vehicles where the victims seem reluctant to describe details or who give inconsistent or conflicting versions of what happened
- Attempts to avoid reporting of fires or minor explosions in residences or storage facilities
- Occupant attempts to restrict access of first responders to areas of the residence or facility, or who attempt to flee before or after the first responders arrive

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Commercial Drivers License students who don't seem interested in finding follow-on employment
- Reports of semi-truck or large vehicle driving training conducted by uncertified individuals – particularly in remote areas such as fields or vacant parking lots at night
- Reports of high-speed, close aboard runs of one or more small boats towards large draft merchant or other vessels restricted in their ability to maneuver – particularly in remote locations near geographic choke points
- Reports of small boats following closely in the wake of a large draft vessel, especially during hours of darkness
- Dangerous maneuvering and other suspicious incidents recently associated with the same two or three individuals
- Launching or retrieval of boats from unusually remote areas
- Boating activities conducted in atypical locations or attempts to loiter near restricted areas
- Reports of gunfire or small explosions by local vessels or coastal residents
- Rescues made from a sunken or stranded vessel where the victims seem reluctant to describe details or who give inconsistent or conflicting versions of what happened
- Requests for specific specialty training, including odd inquiries that are inconsistent with recreational diving
- Demands to learn the advanced skills associated with combat swimming including training with or using rebreathers and diver propulsion vehicles (DPVs), deep diving, conducting kick counts, or receiving extra navigation training
- Rapid progression of Professional Association of Diving Instructors (PADI) training and certifications, particularly if the training is routinely attended by the same students
- Diver training routinely conducted between the same two or three individuals
- Diver training sponsored by groups or agencies that are not normally associated with diving
- Training given by instructors who don't advertise and appear to have little means of visible support, especially those with a history of extremist views
- Diver training conducted in unusually remote or atypical locations or restricted areas
- Threats, coercion, or attempts to bribe trainers for certifications

**Types of technical expertise that terrorists may need to "import"**

Indicators/Reportable Items:

- Efforts to acquire or hire necessary expertise to attack information systems
- Attempts by terrorists to recruit persons with CBRNE relevant expertise

**Technical capability of terrorists to conduct computer network exploitation (CNE) or attacks (CNA)**

Indicators/Reportable Items:

- Affiliations with hackers or hacking groups in the United States or abroad, especially those ideologically aligned with terrorist causes
- Use of Internet or other media or methodologies for mapping and research of prospective information systems by terrorists or their sympathizers
- Attempts to probe information systems by terrorists or their sympathizers
- Acquisition by terrorists of mechanisms and capabilities to penetrate computerized systems to exploit, modify, or deny access to stored data through intruder operations, implanted devices, computer viruses, or malicious codes

**Material**

**Physical and technical characteristics of CBRNE-related materials or weapons sought by, or in the possession of, terrorists**

Indicators/Reportable Items:

- Surveillance of establishments dealing in small arms, ammunition, explosives or dangerous chemicals or materials
- Unusual interest in the backgrounds or associates of employees of establishments where weapons or dangerous materials can be obtained
- Interest in the location, transmission and disposal of CBRNE material or devices
- Purchase of weapons, dangerous materials or specialized or dual use equipment known to be of interest to terrorists using fraudulent means
- Thefts or planned thefts of radiological or toxic material
- Theft or acquisition of hazardous material storage containers

## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Possession or attempted acquisition of instructions on use/handling of toxic chemical and biological substances
- Theft or acquisition of explosives, blasting caps, fuses or certain chemicals used in the manufacture of explosives
- Theft or acquisition of electrical switches
- Presence of castor beans or ricin extract, precatory beans or abrin extract, dimethyl sulfoxide (can be obtained from horse breeders or veterinarians) or nitrobenzene cream
- Sudden, unexplained appearance of unusual illness in hospital emergency rooms

### **Terrorist capability to manufacture CBRNE weapons or materials**

#### Indicators/Reportable Items:

- Evidence of highly-educated, specialized technical personnel such as chemists, biologists, physicists, or engineers isolated from academic or research environments, or evidence of a need for these types of individuals (e.g., request)
- Possession/acquisition of chemicals by quantity and type
- Purchase of portable safety enclosures with chemical fume hood
- Purchase of chemical protective garments and/or masks
- Purchase of portable breathing units
- Purchase of a 30- to 50-liter glass still
- Evidence of completed assembly or device
- Purchase of quantities of Teflon or glass storage containers (3- to 15-liter size)
- Acquisition of established commercial chemical- or biological-testing business or laboratory
- Acquisition or rental of chemical sprayers, spraying vehicles, or aircraft
- Acquisition of various standard laboratory glassware
- Acquisition of portable neutron generators, any type
- Acquisition of nuclear material transporting containers
- Ties to research labs, medical facilities or companies able to purchase CBRNE-type material, equipment, or suspicious or dual-use items
- Evidence of pharmaceutical or agricultural production facilities with apparent change in production mission
- Suspicious deliveries to new customers of chemical or biological material directly from the manufacturer to a self-storage facility, urban residence or rural area
- Evidence of chemical fires, toxic odors, brightly colored stains or rusted metal fixtures in apartments, hotel/motel rooms, self-storage units or garages

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Suspicious inquiries about the location, transmission and disposal of radiological material or devices
- Attempted acquisition of any of the following:

Nerve or Blood Agent Precursors:

- Diethylamine
- 2-ethanethiol HCl
- 2-(diethylamino) ethanol
- Diisopropylamine
- 2-diisopropylamino ethanol
- Methyl phosphonyl dichloride
- Phosphorous oxychloride
- Phosphorous pentachloride
- Phosphorous pentasulfide
- Phosphorous trichloride
- Pinacolone
- Pinacolyl alcohol
- Thiodiglycol

Hydrogen Cyanide Precursors:

- Sodium cyanide
- Sulfuric acid

Mustard Agents:

- Benzene
- Isopropanol
- Sodium fluoride powder
- Methyl phosphonyl dichloride
- Thiodiglycol
- Hydrochloric acid
- Hydrogen chloride gas

Biological Agents:

- Anthrax (Bacillus Anthracis)
- Botulinium toxin
- Yersinia Pestis (Plague)
- Variola Major virus (Smallpox)
- Francisella Tularensis (Tularemia)
- Encephalitis virus (alpha viruses)
- Ricin toxin (or Castor Beans for product)
- Staphylococcal enterotoxins
- Marburg hemorrhagic fever virus
- Coxiella Burnetii (Q Fever)

Biological laboratory equipment:

- Bioreactors/fermenters
- Tissue culture bottles/incubators
- Autoclaves for sterilization
- Separators: centrifugal/cross-flow filters/decanter
- Lyophilizer (freeze dryer)
- Whole body exposure test chamber for aerosol inhalation/exposure testing
- Class III bio-safety cabinets with laminar flow hood
- HEPA filters
- Steam boilers

Nuclear/Radiological Weapons:

Attempted acquisition of nuclear fuels, weapons grade nuclear materials, or radiological sources in any quantities:

Nuclear Fuel:

- Low-enriched uranium

Weapon-Grade Nuclear Material:

- Uranium 233
- Uranium 235
- Plutonium 239

Radiological Sources:

- Cobalt 60
- Cesium 137
- Iridium 192
- Strontium 90

Alternate Nuclear Materials:

- Neptunium
- Americium

**Emerging technologies that terrorist operatives could use to carry out an attack**

Indicators/Reportable Items:

- Plans and capabilities for use of communications jamming equipment
- Extremist access to computer security or computer manufacture businesses and industry
- Extremist plans and moves to acquire new computer hardware, software, and expertise

**Types of equipment/material available to terrorists to facilitate travel, finance and cover**

Indicators/Reportable Items:

- Purchase or presence of tools or equipment (e.g., lamination machines, specialized software, blank forms, documents, etc.) associated with document forgery
- Large quantity of legitimate travel documents lost or stolen

**Intelligence/Security**

**Communications security practices that terrorists might employ**

Indicators/Reportable Items:

- Exclusive use of public telephones
- Speaking in coded or general terms while speaking on the telephone
- Breaking a telephonic conversation flow by calling back on another line
- Frequent change in cell phones or use of "disposable" cell phones
- Conducting periodic examinations of the telephone wire and receiver
- Presence of coded telephone numbers disguised as prices for shopping lists or item serial numbers
- The use of authentication techniques to confirm the identify of the called party
- Sudden discontinued use of a telephone number or email account (on the assumption its use is no longer secure)
- Use of operative courier for message delivery
- Use of steganography (i.e., hiding information by embedding messages within other, seemingly harmless, messages)
- Postmarking letters from a distant post office rather than a local one
- Personal letters received from abroad addressed to P.O. boxes or to other individuals or locations other than the individual's place or residence
- Cloaking or disguising email so messages appear blank (i.e., use of different font or background colors or coded using different language/font settings)
- Email account contains mail in "Drafts" folder but does not transmit email
- Instructions to operatives not to use a method of communication that has been detected by law enforcement or the intelligence community
- Exclusive use of calling cards

## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Exclusive use of cash to purchase calling cards
- Exclusive/excessive use of push-to-talk services
- Use of Voice Over Internet Protocol
- Exploitation of number portability to try to disguise physical location
- Use of personal number services to hide telephone call termination points

### **Methods of cover and concealment**

Indicators/Reportable Items:

- Transport and concealment of CBRNE materials
- Efforts to conceal or disguise potential CBRNE facilities
- Evidence of and details on the protection of high-value materials and unusual security measures
- Fraudulent use of multiple social security numbers
- Shared addresses of multiple businesses with no apparent nexus
- Inability to provide personal background information beyond that contained in documents carried “on-person” or a seemingly practiced set of facts
- No record of travel to the country in which the individual holds a valid passport
- Photos in identity documents that depict the individual without a beard, even though the individual is known to follow religious convention
- Use or presence of forged, fabricated or stolen documents (e.g., exit/entry stamps, birth certificates, passports, visas, identification cards, driver’s licenses, permits, tickets, bank records, student transcripts, etc.)
- Concealment of purchased weapons or materials during transport
- Short-term lease of facilities used by multiple parties
- Meeting location easily accessible by/from a number of roads or means of transportation (e.g., bus or metro rail)
- Conduct of location survey prior to meeting
- Posting of individuals to monitor the location before and after meetings
- Removal of all guards or observers after the participants depart
- Meeting location always on the first floor to facilitate escape
- Meetings never held in a crowded location that would provide cover to security personnel
- Bank account activity indicates structuring



## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Acquisition of, attempts to acquire or manufacture badges, credentials or documents that would allow operatives to impersonate security guards, airline personnel, police officers, military personnel, government officials, or food service workers
- Vehicle has been modified to create a compartment for concealment of materials

### **Methods and tradecraft terrorists might employ to detect counter-terrorist operations and investigations**

Indicators/Reportable Items:

- Conduct of activities consistent with overt or covert intelligence gathering
- Use of surveillance detection techniques enroute to or from the cache site
- Use of surveillance detection and evasion techniques before and after the meeting (e.g., transfer points, indirect routes, taking secondary roads to or from the meeting)
- Use of surveillance detection techniques (e.g., being surveillance conscious and taking indirect routes) by participants before and after meetings

### **Possible counter-measures against law enforcement counterterrorism programs**

Indicators/Reportable Items:

- Exclusive use of foreign bank accounts to obtain cash
- Alternative remittance systems (e.g., hawalas) and unlicensed currency remitters to transfer funds
- Use of security-conscious measures such as counter surveillance techniques
- Increased spending on materials and equipment for reconnaissance and surveillance
- Posting of an armed guard to prevent attacks and to provide advanced warning to meeting participants
- Participants travel alone to the meeting location rather than as a group
- Participants disembark from public or private transportation at a distance from the meeting place
- "Cleaning" of food waste or anything else that would indicate the presence of many people at the location
- Staggering the departure from meetings
- Use of an observation vehicle to provide early warning while enroute to or from a key facility

## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Alteration of vehicle license plates or registrations
- Use of false addresses when applying for identification documentation or travel arrangements
- Lease of space using false identities or fraudulent methods
- Use of couriers to transmit messages, money, weapons, and materials

### **Terrorist activities most vulnerable to counterterrorism measures**

Indicators/Reportable Items:

- Aborted, disrupted or neutralized attempts to attack U.S. interests at home or abroad
- Indications of factions or disagreements within the group

## **Logistics/Infrastructure**

### **Supplies/procurement/storage**

#### **Sources of materials and weapons supplied to terrorists**

Indicators/Reportable Items:

- Contacts or affiliations between terrorists and CBRNE weapons, devices or materials experts
- Communications to or from smuggling sources offering CBRNE weapons, devices or materials
- Evidence of funding transfers between extremist/terrorist organizations and known proliferators of CBRNE weapons, devices or materials

#### **Methods terrorists may use to control, store or distribute weapons and materials**

Indicators/Reportable Items:

- Rental of self-storage space for the purpose of storing chemicals or mixing apparatus
- Procurement of equipment or materials known to be of interest to terrorists
- Purchase and/or alteration of large capacity vans, trucks, or tankers
- Purchase of property by known or suspected terrorists
- Chemical containers discarded in storage unit Dumpsters
- Complaints of unusual fumes, liquids or odors from storage unit customers or neighbors

## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Frequent off-hours visits to storage units, remote storage sites, or abandoned buildings
- Attempts by individuals or small groups of cohorts to check in diving equipment, particularly advanced gear without the required certifications, on commercial flights
- Employment attempts at commercial vehicle dealers, vehicle rental shops, commercial delivery services, security agencies, emergency medical service providers, or freight hauling companies
- Rental vans, delivery vehicles or utility trucks parked in unusual locations such as old barns, fields, vacant warehouses, or other secluded areas

### **Access to large buildings or properties where terrorists could control and/or store weapons or conduct training**

Indicators/Reportable Items:

- Evidence of individuals with no obvious means of income having ownership or leasing of (inactive) licensed businesses, large trucks, (apparently unoccupied) commercial facilities, or storage sites
- Lease of space using false identities or fraudulent methods

### **Mobility**

### **Individuals or organizations facilitating the travel of terrorists, and services they are providing**

Indicators/Reportable Items:

- Use of intermediaries with known or suspected affiliations with human smugglers, forgers, or travel agencies known to facilitate terrorist travel
- Extremist contacts/affiliations with travel service organizations (e.g., airlines, cruise lines or shipping companies), travel agencies, brokers, and document providers
- Financial, ticketing or reservation transactions linking travel facilitators with known or suspected terrorists
- Contacts with terrorist organization members who have historically facilitated travel and documentation arrangements

**Methods of transportation terrorists may use for the movement of personnel and materials**

Indicators/Reportable Items:

- Increase in travel to areas outside day-to-day norms
- Participation in immigration and documentation schemes or alien smuggling
- Use of fraudulent means to obtain travel arrangements
- The purchase or rental of vehicles (especially trucks suitable for moving personnel and/or materials)
- Employment attempts at commercial vehicle dealers, vehicle rental shops, commercial delivery services, security agencies, emergency medical service providers, or freight hauling companies
- Rental vans, delivery vehicles or utility trucks parked in unusual locations such as old barns, fields, vacant warehouses, or other secluded areas

**Finances**

**Indications of terrorist operational funding**

Indicators/Reportable Items:

- Multiple suspicious financial transactions initiating from or terminating at the same location
- Cache(s) of funds, some of which may be held by unwitting associates
- Large wire transfers to or from U.S. financial accounts to accounts in the Middle East or other volatile areas
- State-sponsor financing of terrorist groups
- Establishment or management of financial accounts or channels used by known or suspected terrorists or affiliated organizations
- Bank accounts show indications of structuring
- Ownership in stores that sell stolen, dated, or expired merchandise at inflated prices after tampering with labels
- Fraudulent use of credit cards
- Large deposits / lavish lifestyle that does not align with sales figures from business
- Use of banks or intermediaries with known or suspected terrorist connections
- Account transactions that are inconsistent with past deposits or withdrawals (cash, checks, wires, etc.)
- Transactions involving a high volume of incoming or outgoing wire transfers, with no logical or apparent purpose, that come

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

from, go to, or transit through locations of concern (e.g., sanctioned countries, non-cooperative nations, or sympathizer nations)

- Unexplainable clearing or negotiation of third party checks and their deposits in foreign bank accounts
- Corporate layering; that is, transfers between bank accounts of related entities or charities for no apparent reason
- Wire transfers by charitable organizations to companies located in countries known to be bank or tax havens
- Lack of apparent fund-raising activity (e.g., lack of small checks or typical donations) associated with charitable bank deposits
- Use of multiple accounts to collect funds that are then transferred to the same foreign beneficiaries
- Transactions with no logical economic purpose (e.g., no link between the activity of the organization and other parties involved in the transaction)
- Overlap of corporate officers, bank signatories, or other identifiable similarities associated with addresses, references, and financial activities
- Cash debiting schemes in which deposits in the United States correlate directly with ATM cash withdrawals in countries of concern
- Issuing checks, money orders, or other financial instruments, often numbered sequentially, to the same person or business, or to a person or business whose name is spelled similarly
- Individual owns a business but behaves as if the short term is the priority
- Use of a business account to collect and then funnel funds to a small number of foreign beneficiaries, both individual and business, in a Persian Gulf state
- Use of a business account that would not normally generate the volume of wire transfer activity, into and out of the account, as reported
- Use of a business account to make payments to a brokerage firm
- Procurement of a business that would normally purchase chemical or biological weapons and/or explosives
- Large currency withdrawals from a business account not normally associated with cash transactions
- Funds generated by a business owned by nationals of countries associated with terrorist activity
- Use of multiple individuals to structure transactions under the reporting threshold to circumvent reporting requirements and then funnel funds to a foreign beneficiary
- Same day transactions at the same depository institutions using different tellers

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Shared addresses, which are also business locations, by individuals involved in currency transactions
- Use of cash intensive businesses to disguise the source of funds
- Involvement of multiple nationals of countries associated with terrorist activity acting on behalf of similar business types
- Use of multiple accounts at multiple depository institutions funneling funds to a small number of foreign beneficiaries
- Use of sequentially numbered money orders
- Structuring of money order purchases at multiple locations to circumvent federal Currency Transaction Report requirements and Bank Secrecy Act recordkeeping requirements
- Apparent intent to circumvent wire remittance company's internal requirements for presentation of identification through purchase of money orders in small amounts
- Import/export business acting as an unlicensed remitter to conduct wire transfers
- Individuals/businesses serving as intermediaries in the wire transfer process
- Beneficiaries of wire transfers involving a large group of nationals of countries associated with terrorist activity
- Beneficiaries of wire transfers linked by national origin but residing in multiple nations
- Charity/relief organization linked to the suspects
- Mix of cash deposits and monetary instruments
- Significant deposit amounts to an apparently personal account held by suspect business owner
- Apparent structured, daily deposits to business account
- Wire transfer activity within a short period following deposits
- Beneficiary account in a problematic country
- Currency exchange buying and selling foreign currencies from various countries in the Middle East
- Business account activity conducted by nationals of countries associated with terrorist activity with no obvious connection to the business
- Transactions at a level not commensurate with stated occupations
- Exclusive use of foreign ATM accounts to obtain cash
- Use of banks or intermediaries with known or suspected terrorist connections
- Handling of financial and other material support matters for one or more groups by one or two individuals (commander or team leader)
- Structuring at multiple branches or the same branch with multiple individuals
- Movement of funds through a Financial Action Task Force (FATF)-designated non-cooperative country or territory

## **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Involvement of multiple nationals of countries associated with terrorist activity
- Lifestyle not consistent with known, legitimate sources of income
- Establishment or operation of front organizations to raise or distribute funds for material, recruitment, training, or the sponsorship of travel to the United States by extremists
- Presence at an establishment of blank corporate checks, unusual amounts of food stamps, discount coupons, money orders, or traveler's checks

### **Methods of fund distribution and transportation**

Indicators/Reportable Items:

- Use of messengers to transmit funds
- Unauthorized redirection of funds, by staff members of apparently legitimate organizations, to financial accounts, individuals, or organizations with known or suspected terrorist links
- Changes in patterns of monetary transactions, including trading on financial and commodities markets
- Large wire transfers to or from U.S. financial accounts to accounts of known or suspected terrorists
- Use of express package services like Federal Express, UPS and the U.S. Postal Service to ship funds
- Use of alternate money remittance systems and/or informal banking methods
- Use of commodities to transfer value such as drugs, weapons, cigarettes, diamonds, and gold

### **Counter-measures terrorists might employ to avoid U.S. and international banking and financial regulations**

Indicators/Reportable Items:

- Use of structuring to avoid transaction reporting requirements
- Use of alternate money remittance systems and/or informal banking methods
- Use of couriers to transmit money
- Use of layering to disguise original source of funds
- Maintaining accounts in the name of a nominee
- Use of shell corporations or charities to disguise assets
- Use of offshore banking services
- Over- and under-invoicing
- Use of commodities in lieu of money such as illicit drugs, weapons, cigarettes, diamonds, and gold

- Use of bulk cash shipments

### **Communications**

#### **Methods terrorists may be using to communicate with operatives, support personnel and leadership**

Indicators/Reportable Items:

- Establishment or maintenance of web sites which support terrorist activities and contain anti-U.S. statements
- Use of Internet cafes known to be frequented by extremists
- Websites encouraging terrorist activities
- Websites soliciting recruits for Jihad, ethnic cleansing, etc.
- Websites warning ethnic or religious groups/categories to leave or avoid visiting certain areas
- Use of couriers to transmit messages and electronic media
- High volume of calls to satellite telephones
- Use of websites to disseminate technical information on CBRNE production
- Extensive use of non-landline telecommunications (e.g., Voice over IP)
- Exclusive use of calling cards
- Use of high-frequency radio communications
- Use of media, television, and radio broadcasts

#### **Emerging communications technologies terrorists may be likely to employ**

Indicators/Reportable Items:

- Acquisition of cellular telephones with Internet access capability for emailing and integral cameras for surveillance

#### **Use of the media to advance terrorists' goals to create and maintain fear, manipulate counterterrorism efforts or communicate goals to the world**

Indicators/Reportable Items:

- Use of media to increase the psychological impact of operations
- Use of media to demonstrate the power reach of the terrorist group



## Operations (Terrorist Attacks)

### Objectives of Attack

#### **Objectives and motivations terrorist groups have announced to justify attacks on U.S. interests**

Indicators/Reportable Items:

- Declarations by extremist leaders of Fatwahs or jihads against the United States
- Publishing of a manifesto containing anti-U.S. rhetoric
- Statements by group/national leaders or independent actors containing anti-U.S. rhetoric
- Statements of sympathy towards groups or individuals advocating violence against the United States
- Websites encouraging terrorist activities
- Perception that the United States is responsible for or supported an attack on key terrorist leaders or operatives
- Interest in attack to free colleague(s) in U.S. custody
- Expressions of belief that an attack will influence U.S. policy
- Terrorist leaders broadcast a statement about motivation and desired impact of attack
- Terrorist websites advocating the overthrow of the U.S. government

#### **Types of events or circumstances that could provoke a near-term attack on U.S. or Western targets**

Indicators/Reportable Items:

- Capture or killing of terrorist leaders and/or operatives (especially key leaders)
- Commencement of military tribunals or trials against terror suspects
- Treatment of terrorist suspects in custody, alive or dead, that is perceived to be disrespectful especially to the Muslim faith (e.g., not returning a body for burial along proper Muslim guidelines)
- Activity that is perceived to be anti-Muslim, anti-Arab or pro-Israeli
- Death of known or suspected terrorist in custody
- Upcoming elections
- U.S. Government dismantling of terrorist fund-raising or operational networks

**Factors that are used to measure the success of an attack by terrorist groups against the United States (e.g., psychological impact, financial impact, physical impact)**

Indicators/Reportable Items:

- The assessed ability of a terrorist organization to create or maintain fear in the American/Western public
- Target/attack is projected to create mass panic, confusion, and fear
- Target/attack will create mass casualties

**Type of Attack**

**Types/methods of lethal CBRNE attack terrorists might employ**

Indicators/Reportable Items:

- Presence of weapons such as knives, pistols, rifles, rocket launchers, explosives, poisons, or precursor materials
- Suspicious inquires at agricultural businesses about crop dusting equipment
- Presence or evidence of materials associated with the production of Improvised Explosive Devices (IEDs) and/or suicide vests
- Theft or acquisition of explosives, blasting caps, fuses, or certain chemicals used in the manufacture of explosives
- Theft or acquisition of electrical switches
- Presence of castor beans or ricin extract, precatory beans or abrin extract, dimethyl sulfoxide, or nitrobenzene cream
- Purchase of weapons, dangerous materials, specialized or dual-use equipment known to be of interest to terrorists
- Purchase of SUVs, vans, trucks, or tankers particularly using cash
- Modification of truck or van to handle heavy loads or hazardous materials
- Recent receipts of commercial drivers licenses and permits to haul hazardous and/or toxic materials
- Presence of untreated chemical burns or missing hands/fingers
- Presence of information consistent with explosive devices: firing codes, frequencies, signal modulation types, locations of devices, timing information, etc.
- Thefts of emergency vehicles or utility trucks capable of transporting CBRNE weapons or devices
- Purchase or rental of crop dusting aircraft or crop spraying vehicles
- Purchase or rental of motorized personal aerial vehicles not requiring pilot license to operate

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Arrival of an operative infected with a communicable disease at an operational site, especially with explosive material
- Plans, maps or blueprints that show where IEDs will be placed
- Individuals in possession of information on U.S. food supply sources and pathogens available to contaminate them
- Evidence that suspected operatives intend to target foods that do not require cooking to increase range of effective pathogens
- Indications that terrorist suspects are attempting to target the U.S. water or food supply through employment, theft of uniforms, or identification and access badges
- Evidence that extremists are monitoring or researching water sources, processing or testing procedures at public water sources or treatment facilities
- Indications that terrorist groups are cultivating bacteria that would be resistant to water filtration systems used by U.S. cities

**Types/methods of non-lethal terrorist attacks (to include cyber)**

Indicators/Reportable Items:

- Expressed interest in inflicting psychological damage
- Expressed interest in damaging U.S. economy
- Expressed interest in damaging U.S. infrastructures

**The scope and nature of threats that terrorist groups present to the United States**

Indicators/Reportable Items:

- Terrorist leaders announce plans for attack and state the desired impact of operations

**Types of specialized documentation a terrorist operative would attempt to obtain to execute a specific operation**

Indicators/Reportable Items:

- Attempts to obtain or possession of specialized licenses (e.g., CDL, HAZMAT, or pilot)
- Possession of passes or credentials that allow operatives to impersonate employees (e.g., first responders, security, airline and airport)
- Evidence of a suspected terrorist obtaining or attempting to obtain a license to handle pesticides

- Evidence of a suspected terrorist obtaining or attempting to legitimately or illegally obtain agricultural inspection certification

**Types of activity that would point to the intent of terrorists to use a particular travel mode as a weapon of choice for an attack (e.g., airplane, train)**

Indicators/Reportable Items:

- Suspected terrorists' knowledge and/or evidence of research on the vulnerabilities of the transportation systems in the United States
- Evidence of operational knowledge of transportation of hazardous materials
- Evidence of operational knowledge of airports, schedules, fuel tank storage, runways, command and control systems, etc.
- Evidence of operational knowledge of railways, tunnels, bridges, passengers, and stations
- Evidence of operational knowledge of transportation, highways, trucking, busing, critical chokepoints, border crossings, maintenance facilities, etc.
- Evidence of a suspected terrorist obtaining or attempting to obtain training as an air traffic controller

**Plans/Tactics**

**Indications that terrorist groups are planning imminent or near-term attacks on U.S. interests**

Indicators/Reportable Items:

- Increase in number of "friends/family" visiting residence of suspected operative at odd times or for odd durations
- Increased tempo of extremist training or in the movement of personnel and equipment
- Meetings between commanders or other leadership to review the operational plan and alternatives
- Communications notably increase/decrease between operatives, support, and leaders
- Individual has no concern for the future (e.g., does not ask for change or receipts when purchasing or renting items)
- Travel of a known or suspected commander out of the area where reconnaissance has been conducted
- Purchase of a one-way ticket in cash

## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Movement of personnel, equipment, and weapons to the operational area
- Conduct of a final reconnaissance to ensure no significant changes in the operational area have occurred
- Letters/notes explaining the operation; saying goodbye, etc.
- Religious rituals are performed that are associated with martyrdom
- Terrorist suspects in possession of information consistent with explosive devices: firing codes, frequencies, signal modulation types, locations of devices, timing information, etc.

### **Weapons, manpower and method of delivery that terrorists may use in an attack**

Indicators/Reportable Items:

- Vehicles being purchased, leased, stolen, or rented by terrorist suspects and altered for possible operations
- Acquisition of containers capable of holding explosive, chemical, or biological weapons
- Acquisition of precursor materials/ingredients for explosives, chemical, or biological weapons
- Acquisition of specialized weapons (e.g., assault or sniper rifles) or CBRNE materials
- Suspects survey rail, flight, shipping schedules, operations, and transport nodes
- Suspects survey catering companies, food supply, or agricultural entities
- Rhetoric or communication code refers to phrases that may indicate source, direction, or method of attack

## Targeting

### **Likely target(s) of terrorist attack**

Indicators/Reportable Items:

- Presence in a residence or vehicle of hardcopy or electronic materials (e.g., photographs or text descriptions/biographies) of important U.S. officials, facilities, security points, etc.
- Presence of detailed diagrams and notes about buildings, bridges, ports, airfields, tunnels, etc.
- Tests of security at airports, railway terminals, or border crossings and other high priority targets
- Details on personal security forces and operating procedures

## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Activities to collect information about important persons such as their residence, work schedule, travel routes, family, acquaintances, physicians, vehicles, free time pursuits and venues, etc.
- Succession of detailed reconnaissance activities by local networks
- Theft of official uniforms or vehicles that would allow access to restricted areas
- Use of Internet or other media or methodologies for surveillance, mapping and research of prospective infrastructure and physical targets
- Surveillance of targets such as dams, airfields, tunnels, bridges, nuclear facilities, government agency headquarters, or other symbolic sites
- Stated animosities towards specific individuals or groups
- Use of almanacs and other reference materials that may signal operational intentions
- Communications chatter using general terms or coded language which points to categories of targets and their location in the United States or abroad
- Operational testing or reconnaissance in venues associated with targets of interest (e.g., airlines, mass transit, transportation infrastructure, energy infrastructure, or tourist attractions)
- Interest by known or suspected terrorists in government personnel and important personalities
- Interest by known or suspected terrorists about strategic buildings, important establishments, military bases, airports, seaports, border crossing points, embassies, and radio and television stations
- Interest by known or suspected terrorists about Western interests overseas (oil refineries, embassies, U.S. businesses, etc.)
- Attempts to recruit informants or agents who are knowledgeable about persons or facilities, including employees at border crossings, airports, and seaports
- Theft of plans or blueprints associated with strategic sites
- Surveillance or testing of security at active oil pipelines
- Interest by known or suspected terrorists in medical research labs that handle Biological Safety Level (BSL) 3 and 4 containment level materials
- Interests by known or suspected terrorists in symbols of American power or pride: monuments, military bases, government buildings, famous tourist attractions and cities
- Interests by known or suspected terrorists in American symbols of religion: synagogues, Jewish cultural centers, etc.
- Attempts to compromise the integrity of a system—especially systems that control utilities, government sites, financial records, information, or communications

- Interest by known or suspected terrorists in commercial targets such as theme parks or sporting events
- Interest in port schedules
- Interest in ships/freighters carrying explosive cargo
- Interest in ferry or cruise ship itineraries and port schedules

## **Timing/Sequencing**

### **Current phase of execution for attacks (e.g., planning, reconnaissance, rehearsal, deployment)**

Indicators/Reportable Items:

- Planned or attempted travel of a known or suspected operational commander or operatives to the United States or areas with a large U.S. or Western presence
- Appearance of a known or suspected operational commander or new operatives in the United States or areas with a large U.S. or Western presence
- Recruitment of volunteers
- Concentration of operatives to a particular location, region, or pending dramatic events
- Changes (dramatic increases or decreases) in communications among or between terrorists and/or state sponsor governmental or political components
- Leasing of apartments in the United States or close to U.S. facilities overseas under false identities
- Recent arrival of small groups (3-5 members) in apartments, whose presence and identities are not known to landlord
- Increased or decreased frequency of meetings or contact between suspected members of extremist groups
- Movement of personnel, equipment, and weapons to the operational area
- Recent arrival of new or previously unidentified associates of subjects
- Rehearsals of operational tactics in areas or venues similar to that of the real target (same as below)
- Spikes in purchases of antidotes to biological or chemical agents
- Conduct of a final reconnaissance to ensure no significant changes in the operational area have occurred
- Arrival of additional operatives and senior experts (especially with specialties such as explosives knowledge) to prepare methods of attack
- Testing of arms or other types of weapons, such as explosives
- Increased visits to mosque for meeting or prayers
- Ritual cleansing

**Types of financial activity that may indicate an imminent attack**

Indicators/Reportable Items:

- Sudden, unexplained changes in financial transactions including closure of recently established accounts
- Transactions are operationally oriented: truck rentals, airline ticket purchase, or acquisition of materials of concern are acquired

**Operational Reconnaissance or Surveillance**

**Terrorist group reconnaissance or surveillance of potential targets**

Indicators/Reportable Items:

- Suspicious behavior, such as staring or quickly looking away from personnel or vehicles entering or leaving designated facilities or parking areas
- Foot surveillance involving two or three individuals working together
- Mobile surveillance using bicycles, scooters, aircraft, and other vehicles
- Prolonged static surveillance using operatives disguised as panhandlers, food vendors, news agents, street sweepers, etc.
- Discreet use of still cameras, video recorders or note taking
- Purchase and use of covert surveillance equipment
- Use of multiple sets of clothing, identification, or the use of sketching materials
- Unusual or prolonged interest in security measures (personnel, entry points, access controls, perimeter barriers, etc.) of facilities known to be of interest as targets
- Observation of security drills or procedures
- Sequence of detailed reconnaissance activities by local networks
- Videotaping or photographing of tunnels, bridges, transportation facilities, gas sites, houses of worship, government facilities, religious schools, etc. outside of normal tourist behavior
- Asking questions of security personnel about security procedures, foot traffic, etc.
- Individual approaches a building or site and suddenly retreats when a security checkpoint or personnel are observed



## Operational Security

### Methods of operational security terrorists may use to protect operations and personnel

Indicators/Reportable Items:

- Details on personal security forces and operating procedures of suspected groups
- Providing false identities of sponsors or associates or false details of plans while in the United States
- Presence of coded telephone numbers disguised as prices for shopping lists or item serial numbers
- Use of authentication techniques to confirm the identify of the called party
- Conversations begin using pre-scripted dialogue
- Nature of previously coded or cryptic conversations and messages suddenly changes to reveal details in apparent attempt at disinformation
- Use of cryptography to protect operational information and to protect financial and operational records stored on computer
- Use of Internet cafes known to be frequented by terrorists
- Use of prearranged verbal or physical authentication or safety signals between meeting participants (e.g., the use of phrases, keys, prayer beads, newspapers, scarves or other articles of clothing)
- Use of couriers or messengers to move items, messages, and funds to avoid detection and prosecution
- Boarding or disembarking at secondary rather than primary stations, even though primary stations are closer to start points or end locations
- Placing luggage in a different car or compartment than the one being occupied
- Avoidance of travel in low-traffic areas
- Responses to questions from security personnel appear practiced
- Alteration of vehicle color or identifying features before or after an operation
- Individual stays at a hotel, refuses maid service and asks for a room with a view of a particular landmark; room may be a meeting place
- Operatives acquire an armored car
- Individuals in possession of uniforms (military, clerical, medical, civil service, law enforcement) that do not match their stated profession
- Evidence of terrorists creating weapons that can be smuggled onto aircraft and through security points without detection

**Denial and deception tactics to support imminent operations**

Indicators/Reportable Items:

- Cache(s) of personal identification documents stored in unusual locations or containers
- Possession of identification documents bearing more than one identity
- Use of falsified documents
- Reports of cooperation between individual journalists or authors and terrorist group leaders
- Information suggesting attempts to garner an exclusive reporting agreement between a media entity and terrorist group leadership
- Evidence of publishing agreements made on behalf of the terrorist group such as biographical works, manifestos, group histories and/or archives, etc.
- Publications, documents, video or audio recordings that appear to contain draft or final works of a biographical nature dealing with senior members of a terrorist group, its cohorts, or the movement in general
- Reports of efforts involving the production of films or documentaries related to senior terrorist group members
- Reports of assistance provided by journalists or others in transferring media or publications to support terrorist group statements or communiqués
- Information suggesting trends, patterns, or bias in media reporting that deals with a particular terrorist group or movement
- Reports of cooperation and collaboration between foreign government officials, NGO leadership, celebrities, and/or business or community leaders and media personnel with respect to terrorist group reporting
- Information claiming a habitual pattern of inaccurate, and/or exaggerated or alarmist reporting concerning a terrorist group, on the part of a foreign security or intelligence service and/or media entity
- Evidence suggesting trends or patterns in terrorist-related hoaxes and/or threat reporting
- Trends or patterns in terrorist suspect statements made during surveillance
- Information suggesting pre-rehearsed responses to questions related to terrorist plans and/or capabilities during media statements or interviews, detainee and/or prisoner interrogations
- Evidence suggesting deliberate deception attempts, (e.g., planted evidence, false broadcasts, attack feints, contrived source reporting)
- Evidence suggesting trends or patterns of disinformation-related postings or similar propaganda offerings on the Internet

## UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Reports of terrorist disinformation efforts directed at (or attempting to exploit) religious proselytizing, observances, and/or community ministry, outreach activities, political functions, or electoral activities
- Information suggesting terrorists are attempting to use a disinformation campaign as a means of distraction from an actual attack
- Information suggesting terrorists are attempting to overload intelligence efforts with bogus threat reporting in a deliberate attempt to desensitize security forces
- Evidence suggesting U.S. or foreign military personnel are attempting to aid terrorists in their deception efforts
- Reports of attempts to establish dummy sites or fake facilities to mislead intelligence efforts
- Information suggesting a pattern of sensitive equipment or material purchasing inquiries that provide little or no information that would normally be expected for a legitimate business transaction
- Information indicating terrorist participants in high interest activity, such as diver training, are not concerned about observation and/or disclosure
- Evidence suggesting terrorists are attempting to "manufacture" an attack or other newsworthy event

### **Movement to/from Target: Staging**

#### **Transportation means/nodes/routes terrorist operatives may use to attack U.S. interests**

Indicators/Reportable Items:

- Extremist contacts or affiliations with transportation officials or employees (shipping lines, airlines, port or station officials)
- Statements regarding specific transportation methods or targets by terrorist leaders/operatives
- Surveillance or testing at border crossings

#### **Staging areas for attack(s)**

Indicators/Reportable Items:

- Concentration of operatives in a particular location or region
- Purchase of real property by known or suspected terrorist operatives
- Delivery of chemicals or biological material directly from the manufacturer to a self-storage facility or unusual deliveries of such material to residential or rural areas (recent or new customers)

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Chemical fires, unusual or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel/motel rooms, self-storage units or garages

**The point/methods of entry to the United States that are least secure and most attractive to terrorist organizations**

Indicators/Reportable Items:

- Surveillance, testing at specific border crossing areas

## **Criminal Activities (non-operations)**

### **Inside the Continental United States**

#### **Illegal activities terrorists may conduct in the United States to support themselves**

Indicators/Reportable Items:

- Drug manufacturing, smuggling, and distribution
- Identity theft for profit
- Credit-card, insurance, welfare, and food-stamp fraud
- Counterfeit merchandise schemes
- Interstate smuggling
- Ownership in stores that sell stolen, dated, or expired merchandise after tampering with labels

### **Outside the Continental United States**

#### **Illegal activities terrorists may engage in abroad to support themselves**

Indicators/Reportable Items:

- Foreign law enforcement arrests of terrorist suspects (cite specifics of arrest warrants)
- Foreign prosecutions of terrorist suspects (cite criminal counts)
- Foreign press reports of alleged terrorist criminal activities
- Arrangement of marriages to facilitate and expedite foreign citizenship for individuals who would not otherwise be eligible or to avoid legal requirements

### **Nature/Purpose of Illegal Acts**

#### **Purposes (e.g., finance, intelligence, weapons acquisition) that terrorist criminal activities may be supporting**

Indicators/Reportable Items:

- Theft or smuggling of specialized materials, documents, explosives, or contraband
- Ownership in stores that sell stolen, dated, or expired merchandise after tampering with labels

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

- Bribery of officials to obtain permits, licenses, contracts, or to obstruct investigation
- Manuals or instruction documents describing specialized criminal techniques (e.g., theft, forgery, identity falsification, illegal weapons manufacture, or acquisition)

FOR OFFICIAL USE ONLY



FOR OFFICIAL USE ONLY