Terrorist Threats to the U.S. Homeland

Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators

Department of Homeland Security
Washington, DC 20528

January 7, 2005

SUBJECT: **Terrorist Threats to the U.S. Homeland Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators**

FOR: **Critical Infrastructure Owners and Operators, Information Sharing and Analysis Centers (ISACs), Security Managers, and Facility Operators**

This Terrorist Threats to the U.S. Homeland Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators (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 resources of our *critical infrastructure partners* to assist in recognizing activities or conditions that may be indicative of terrorist activity. Critical infrastructures are on the "front line" in the war against terror and therefore have a key role as primary sources of threat-related information. This timely and relevant information is critical to the identification of possible terrorist and terrorist-related activity. The TTRG identifies common indicators and patterns that may be associated with terrorist threats to the nation's critical infrastructure. This guide also encourages reporting of relevant indicators and patterns to law enforcement and homeland security officials.

The TTRG is intended to complement the reader's knowledge of possible indicators of terrorist activity which may be encountered during the course of normal operations. It is not a request for intelligence collection, and does not provide the authority to conduct law enforcement or intelligence-related operational activities. Recipients are encouraged to consult with their legal counsel as to any questions regarding the scope of their legal authorities.

I want to personally thank you for your time and effort in reporting actual or potential threats to critical infrastructures within our Homeland. Information received by DHS and FBI—from all sources including critical infrastructure owners and operators—will be reviewed, analyzed, and disseminated as appropriate to our mission partners via approved warning dissemination channels.

Sincerely,

//S
Frank Libutti
Under Secretary
Information Analysis and Infrastructure Protection
Department of Homeland Security

PRIVACY NOTICE

Introduction

This Reporting Guide is provided as a public service by the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).

Information Collected and Stored Automatically

Information related to the person or organization making a report pursuant to this guide shall be collected and stored by DHS and FBI, as follows:

- For reports submitted by telephone: the telephone number, the date and time of the telephone call, and the identity of the individual and/or organization submitting the report;
- For reports received by e-mail: the e-mail address and its domain, the date and time of the e-mail, and the identity of and any other identifying information about the individual and/or organization submitting the report; and
- For reports submitted electronically (via HSIN, the Homeland Security Information Network): the name of the domain and IP address from which you accessed HSIN, the type of browser and operating system used to accessed HSIN, the date and time you accessed HSIN, the internet address of the website from which you linked to HSIN; and the web pages you visited within HSIN.

This information is primarily collected for statistical analysis, and will be used for purposes such as assessing what information is of priority interest, determining technical design specifications for the reporting system, and identifying system performance and/or problem areas. In certain circumstances, however, DHS or FBI may take additional steps to identify you based on this information and may share this information, including your identity, with other government agencies.

Security Monitoring on HSIN

For the security of HSIN, and to ensure that HSIN services remain available to all users, all network traffic on HSIN is monitored in order to identify unauthorized attempts to upload or change information, or otherwise to cause damage or conduct unauthorized or criminal activity. To protect HSIN services from unauthorized use and to ensure that those services are functioning properly, individuals using those services are subject to monitoring of all activities on those services and recording of this information by personnel authorized to do so by DHS or FBI. Anyone using HSIN expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible unauthorized or criminal activities, evidence of the monitoring will be provided to appropriate officials for action. Unauthorized attempts to upload or change information, or otherwise cause damage to HSIN, are strictly prohibited and may be punishable under applicable federal law.

Disclaimer of Endorsement

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government.

Terrorist Threats to the U.S. Homeland: Reporting Guide
For Critical Infrastructure and Key Resource Owners and Operators

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). The Department of Homeland Security and the Federal Bureau of Investigation shall remain the sole Federal Agency Custodians of Record for this reporting guide, retaining both possession and control of this document for FOIA purposes. 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, homeland security, and critical infrastructure personnel, without prior approval of an authorized DHS or FBI official. To obtain approval, please contact the National Infrastructure Coordination Center at 202-282-9201. Refer FOIA requests for this document or portions of this document to the Department of Homeland Security or the Federal Bureau of Investigation. **Information in this document is NOT for general public dissemination.**

This Reporting Guide is intended to complement the reader's knowledge of possible indicators of terrorist activity which may be encountered during the course of normal operations. It is neither a request for intelligence collection nor authority for the conduct of law enforcement or intelligence activities. Recipients are encouraged to consult with their legal counsel as to any questions regarding the scope of their legal authorities.

Nothing in this Reporting Guide shall give directly or indirectly to any party any enforceable benefit, privilege, right, or right of action against the United States Government, against any Agency of the United States Government, or against any United States Government official. None of the contents of this document shall serve as a basis to enhance the provision or enforcement of any right, privilege, benefit or action by the United States Government otherwise or elsewhere provided.

Table of Contents

Introduction

This Terrorist Threats to the U.S. Homeland Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators (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 resources of our *critical infrastructure partners*, in recognizing activities or conditions that may be indicative of terrorist activity. State and local organizations and the owners and operators of our nation's critical infrastructure are on the front line in the war against terror and therefore have a critical role as primary sources of threat-related information. Timely and relevant information from the "front lines" is critical to the development of insights into terrorist plans and intentions, and subsequent disruption of their operations. **This guide incorporates and builds upon the joint FBI / DHS Memo *Suspicious Activity Reporting Criteria for Owners and Operators dated 3 August 2004.* It identifies common indicators and patterns that <u>may</u> be associated with terrorist threats to all sectors of the nation's critical infrastructure. If warranted by threat information, DHS may update this guide with appendices to provide additional sector-specific guidance.**

Threat warning information products prepared as a result of the use of this guide will be published and disseminated through established DHS and FBI channels.

Reporting Guidance

DHS and FBI encourage recipients of this Reporting Guide, including the Sector Coordinating Councils (SCCS) and Information Sharing and Analysis Centers (ISACs), 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 National Infrastructure Coordinating Center (NICC), a sub-element of the Homeland Security Operations Center (HSOC). The NICC can be reached via telephone at 202-282-9201** or by email at TTRGReporting@dhs.gov (which is automatically forwarded to both the NICC and HSOC).

Each report submitted should include the date, time, location, type of activity, potential target, number of people and type of equipment or material used for the activity, the name of the submitting organization and a designated point of contact (POC).

The DHS and FBI have compiled the following list to assist our homeland security partners in recognizing and reporting potential terrorist activities. The information is organized into four general areas:

- Surveillance, Probing, and Reconnaissance of Critical Infrastructure
- Attempts to Gain Unauthorized Access to Critical Infrastructure
- Attempts to Gain Unauthorized Access to Materials or Training
- Use of Materials or Financing to Support Terrorist Activity

Surveillance, Probing, and Reconnaissance of Critical Infrastructure

- Report attempts to test or conduct reconnaissance of security operations at critical infrastructure / key resource facilities, high profile venues or sector-specific events.

- Report any persons showing uncommon interest in security measures or personnel, entry points or access controls, or perimeter barriers such as fences or walls.

- Report any persons showing uncommon interest in critical infrastructure / key resource facilities, networks, or systems (e.g. photographing or videotaping assets).

- Report all suspicious attempts to recruit employees or persons knowledgeable about key personnel or critical infrastructure / key resource facilities, networks, or systems.

- Report any persons loitering for no apparent purpose near critical infrastructure / key resource facilities who do not fit the surrounding environment, such as individuals wearing improper attire for conditions not normally present in the area.

    - Note any responses to questions posed by security personnel from such individuals which appear practiced.

    - Note possession by such individuals of uniforms (military, clerical, medical, civil service, law enforcement) which do not match their stated profession.

- Report pedestrian surveillance near critical infrastructure / key resource facilities involving any surveillance activity of sensitive operations, including photography, videotaping, or extensive note-taking / use of audio recorder (regardless of the number of individuals involved), or mobile surveillance by cars, trucks, motorcycles, boats or small aircraft.

    - Note suspicious behavior, such as staring or quickly looking away from personnel, unexplained vehicle movement, or sudden movement by personnel or vehicles when approached or observed by security personnel.

    - Note apparent foot surveillance involving two or more individuals working together, and prolonged static surveillance by personnel performing apparent work functions for unusually long durations.

    - Note mobile surveillance using bicycles, scooters, cars, aircraft, watercraft, or other vehicles. Where possible, attempt to identify make / model / license numbers.

    - Note secretive use of still cameras, video recorders, sketching, or note-taking.

        - Note videotaping, photography, or sketching of critical infrastructure facilities not normally associated with normal tourist interest or behavior.

- Note unusual or prolonged interest in security measures (personnel, entry points, access controls, perimeter barriers, etc.) of facilities.

    - Note inquiries to security personnel about security procedures, access points, foot traffic patterns, and security technologies in place.

- Note observation of security drills or procedures.

- Note repeated attempts at surveillance by the same individual or groups of individuals, particularly attempts involving multiple sets of clothing within the same day, the use of different vehicle, or the use of different identification documents.

- Report all stated threats to critical infrastructure facilities or sector-specific events received via e-mail, letter, telephone, or website postings, particularly repeated threats from different sources or threats apparently designed to elicit a security response.

    - Report all threats indicating a sophisticated knowledge of critical infrastructure facility structure, systems operation, or personnel structure.

- Report unauthorized attempts to probe or gain access to proprietary information systems, particularly Supervisory Control and Data Acquisition (SCADA) systems, to include the use of social engineering techniques (e.g., attempts by unauthorized individuals to gain physical or electronic (e.g., password) access to systems via impersonation of authorized functions or personnel).

- Report 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.

- Report small boats following closely in the wake of a large draft vessel, especially during hours of darkness.

Attempts to Gain Unauthorized Access to Critical Infrastructure

- Report any theft of or missing official company identification documents, uniforms, credentials, or vehicles necessary for accessing critical infrastructure / key resource facilities or sector-specific events.
    - Note acquisition of, attempts to acquire or manufacture badges, credentials or documents that would allow operatives to impersonate company officials or staff, security guards, airline personnel, police officers, military personnel, government officials, or food service workers.
    - Note acquisition of, attempts to acquire or manufacture certifications by individuals with no apparent legitimate purpose (e.g., agricultural inspection certification, HAZMAT license).
    - Note use 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) to support access to critical infrastructure / key resource facilities or sector-specific events, or acquisition of credentials for the same purpose.
    - Note recovery of any abandoned or stolen official vehicles, particularly if missing registration documents or vehicle identification number (VIN).
- Report any theft, unauthorized purchase, or unauthorized disclosure of plans, blueprints, engineering diagrams, alarm system schematics, or similar physical security-related or sensitive information related to a facility with critical infrastructure / key resource facilities and systems.
- Report any theft, unauthorized purchase, or unauthorized disclosure of pictures or drawings of critical infrastructure / key resource facilities or systems.
- Report boating activities conducted in atypical locations or attempts to loiter near restricted areas.

Attempts to Gain Unauthorized Access to Materials or Training

- Report attempts by an unauthorized and / or unlicensed individual or group to obtain or initiate the production of precursor chemicals and agents, including advanced nerve agents, infectious bacterial and viral agents, biological toxins, or nuclear / radiological devices (see material list on pages 12-13).

Facilities Associated with Dangerous Materials:

- Report unusual purchases of laboratory equipment and requests for access to laboratories for no apparent purpose, or for purposes at odds with the type and sophistication of equipment requested.
    - Note use of fraudulent documents or credentials to support purchase or access requests.
- Report sudden, unexplained changes in production by chemical, pharmaceutical or agricultural facilities.
- Report unusual security procedures associated with a laboratory, pharmaceutical, or agricultural facility, particularly security beyond levels normally associated with the stated or apparent purpose of the facility.
- Report unusual or unexplained interest in medical research labs that handle Biological Safety Level (BSL) 3 and 4 containment level materials.
- Report unusual interest in the backgrounds or associates of employees of establishments where dangerous materials can be obtained.
- Report surveillance of establishments dealing in small arms, ammunition, explosives or dangerous chemicals or materials.
- Report suspicious inquires at agricultural businesses about crop dusting equipment.

Acquisition of Dangerous Materials:

- Report theft or unusual / unauthorized purchase attempts of potentially toxic biological cultures, microorganisms, or dual use biological material.
- Report theft or unusual / unauthorized purchase attempts of crop toxins, insects, or livestock disease pathogens that could impact national agriculture.
- Report theft or unusual / unauthorized purchase of castor beans or ricin extract, precatory beans or abrin extract, dimethyl sulfoxide (can be obtained from horse breeders or veterinarians) or nitrobenzene cream.

- Report theft or unusual / unauthorized purchase of antidotes to poisons, particularly in large or unusual quantities, or for rare or unusual poisons.

- Report theft or unusual / unauthorized purchase of equipment, components and related materials for the design and / or fabrication of nuclear / radiological devices.

- Report theft or unusual / unauthorized acquisition of containers capable of holding explosives, lethal chemical agents, or biological agents and toxins.

- Report theft or unusual / unauthorized acquisition of explosives, blasting caps, fuses or certain chemicals used in the manufacture of explosives.

- Report theft or unusual / unauthorized acquisition of electrical switches.

- Report theft or unusual / unauthorized acquisition of any of the following chemicals or biological materials:

  Nerve or Blood Agent Precursors:
  - Diethylamine
  - 2-ethanethiol HCl
  - 2-(diethylamino) ethanol
  - Diisoproplyamine
  - 2-diisoproplyamino 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:

- Bacillus Anthracis (Anthrax)
- 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)

- Report use of fraudulent documents or credentials in attempts to acquire any of the above listed materials.

Indicators of Use of Dangerous Materials:

- Report sudden, unexplained illness of livestock herds or human population in a local area, particularly that involving viruses or unusual disease(s) not normally associated with the area (e.g., malaria in dry or non-tropical climate).

- Report detection or treatment of unexplained chemical burns or chemical exposure injuries, particularly if associated with vague, irrational, or deceptive explanations.

  - Note unusual burns or illness in animals which may be indicative of unauthorized materials or biological testing.

- Report use of facilities (e.g., warehouses, self-storage rentals) to store unusual or unexplained quantities of chemicals, HAZMAT, or biological material.

- Report unusual, unexplained, or unauthorized use or rental of chemical sprayers, spraying vehicles, or aircraft.

  - Note evidence of unusual or unauthorized attempts to obtain a license to handle pesticides.

- Report suspicious purchase or rental of motorized personal aerial vehicles (e.g., ultralights) not requiring pilot license to operate.

- Report suspicious deliveries to new or non-traditional customers of chemical, radiological or biological material directly from the manufacturer to a self-storage facility, urban residence or rural area.

- Report unusual chemical containers (type / quantity) discarded in storage unit Dumpsters.

- Report complaints of unusual fumes, liquids or odors from storage unit customers or neighbors.

- Report frequent off-hours visits to storage units, remote storage sites, or abandoned buildings.

- Report rental vans, delivery vehicles or utility trucks parked in unusual locations such as old barns, fields, vacant warehouses, or other secluded areas.

- Report 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.

    - Note attempts to avoid reporting of fires or minor explosions in residences or storage facilities.

    - Note occupant attempts to restrict access of first responders to areas of a residence or facility, or who attempt to flee before or after the first responders arrive.

- Report evidence of chemical fires, toxic odors, brightly colored stains or rusted metal fixtures in apartments, hotel / motel rooms, commercial offices, self-storage units or garages.

- Report possession or acquisition of the following materials by persons with no apparent knowledge or skills related to their use:

    - Portable safety enclosures with chemical fume hood
    - Chemical protective garments and / masks
    - 30- to 50-liter glass stills
    - Quantities of Teflon or other glass storage containers (particularly 3- to 15-liter size)
    - Established commercial chemical- or biological-testing business or laboratory
    - Chemical sprayers, spraying vehicles, or aircraft
    - Various standard laboratory glassware
    - Portable neutron generators, any type
    - Nuclear material transporting containers

Attempts to Acquire Specialized Training or Expertise:

- Report unauthorized or unusual attempts to obtain or conduct organized training in security concepts, conventional military weapons and tactics and CBRNE weapons.

- Report unauthorized or unusual attempts to obtain specialized training concerning explosives, such as explosives, firearms, survival, flight school or defensive driving.

- Report semi-truck or large vehicle driving training conducted by uncertified individuals – particularly in remote areas such as fields or vacant parking lots at night.

  - Report lack of interest by Commercial Drivers License students in finding follow-on employment.

- Report unusual interest in training in surveillance, weapons, intelligence-gathering, or counter-surveillance or counter-intelligence techniques.

- Report attempts to threaten, coerce, or bribe trainers for certifications or licenses.

Use of Materials or Financing to Support Terrorist Activity

- Report unusual purchases of tools or equipment (e.g., lamination machines, specialized software, blank forms, documents, etc.) associated with document forgery.

- Report evidence of funding transfers between federally listed organizations and known suppliers of CBRNE weapons, devices or materials.

- Report multiple suspicious financial transactions initiating from or terminating at the same location.

- Report cache(s) of funds, some of which may be held by unwitting associates.

- Report establishment or management of financial accounts or channels used by known or suspected terrorists or affiliated organizations.

    - Note bank accounts which show indications of structuring.

- Report transactions involving a high volume of incoming or outgoing wire transfers, with no logical or apparent purpose, that come from, go to, or transit through locations of concern (e.g., sanctioned countries, non-cooperative nations, or sympathizer nations).

- Report unexplainable clearing or negotiation of third party checks and their deposits in foreign bank accounts.

- Report corporate layering; that is, transfers between bank accounts of related entities or charities for no apparent reason.

- Report wire transfers by charitable organizations to companies located in countries known to be bank or tax havens.

- Report lack of apparent fund-raising activity (e.g., lack of small checks or typical donations) associated with charitable bank deposits.

- Report use of multiple accounts to collect funds that are then transferred to the same foreign beneficiaries.

- Report transactions with no logical economic purpose (e.g., no link between the activity of the organization and other parties involved in the transaction).

- Report use of a business account to collect and then funnel funds to a small number of foreign beneficiaries, both individual and business.

- Report use of a business account that would not normally generate the volume of wire transfer activity, into and out of the account, as reported.

- Report use of multiple individuals to structure transactions under the reporting threshold to circumvent reporting requirements and then funnel funds to a foreign beneficiary.

- Report use of multiple accounts at multiple depository institutions funneling funds to a small number of foreign beneficiaries.

- Report structuring of money order purchases at multiple locations to circumvent federal Currency Transaction Report requirements and Bank Secrecy Act recordkeeping requirements.

- Report apparent intent to circumvent wire remittance company's internal requirements for presentation of identification through purchase of money orders in small amounts.

- Report import / export businesses acting as an unlicensed remitter to conduct wire transfers.

- Report business account activity conducted by nationals of countries associated with terrorist activity with no obvious connection to the business.

- Report movement of funds through a Financial Action Task Force (FATF)-designated non-cooperative country or territory.

- Report use of alternate money remittance systems and / or informal banking methods, or commodities to transfer (e.g., drugs, weapons, cigarettes, diamonds, and gold).