



Federal Bureau of Investigation



Homeland Security

August 3, 2004

SUBJECT: Suspicious Activity Reporting Criteria for Infrastructure Owners and Operators

FOR: Information Sharing and Analysis Centers (ISACs), State Homeland Security Advisors, Government First Responders, Security Managers, and Facility Operators

DHS and FBI encourage recipients of this memorandum to report information concerning suspicious or criminal activity to their local FBI Joint Terrorism Task Force (JTTF) – the regional phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm> – and the Homeland Security Operations Center (HSOC) or the National Infrastructure Coordination Center (NICC), a sub-element of the HSOC in support of the private sector and critical infrastructures. The HSOC can be reached via telephone at 202-282-8101 or by email at HSCenter@dhs.gov; and the NICC/HSOC can be reached via telephone at 202-282-9201 or via email at NICC@dhs.gov.

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

Overview

DHS and FBI request that the owners and operators of the nation's critical infrastructure/key resource facilities (see Appendix), provide reporting to the above offices on the following types of suspicious activities potentially indicative of pre-operational terrorist planning:

Surveillance/Probing Activity

- 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 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.
- Report all suspicious attempts to recruit employees or persons knowledgeable about key personnel or critical infrastructure/key resource facilities, networks, or systems.
- Report any theft, purchase, or suspicious means of obtaining plans, blueprints, 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 discovery of documents (particularly foreign language products) containing pictures or drawings of critical infrastructure/key resource facilities or systems.
- Report any persons near critical infrastructure/key resource facilities who do not fit the surrounding environment, such as individuals wearing improper attire for conditions or not normally present in the area (such as, homeless persons, street vendors, demonstrators, or street sweepers).
- 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.

Threats/Warnings

- Report all threats/warnings that could affect the reliability and operation of the nation's critical infrastructures/key resources.
- Report discoveries of website postings which make violent threats specific to critical infrastructures or sector specific events.

For comments or questions related to the content or dissemination of this memorandum, please contact the DHS/Information Analysis and Infrastructure Protection Directorate's Requirements Division at DHS.IAIP@DHS.GOV.

APPENDIX

CRITICAL INFRASTRUCTURES AND KEY RESOURCE FACILITIES¹

Critical Infrastructures

- Banking and Finance
- Chemical
- Defense Industrial Base
- Electric Power
- Emergency Services
- Food/Agriculture
- Information Technology
- National Monuments and Icons
- Oil and Natural Gas
- Postal and Shipping
- Public Health
- Telecommunications
- Transportation (Rail/Mass Transit, Maritime, Aviation, Highway)
- Water

Key Resource Facilities

- Commercial Facilities
- Dams
- Government Facilities
- Nuclear Reactors/Materials

¹ Under the Homeland Security Act, which references the definition in the USA PATRIOT Act, the term “critical infrastructure” means “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” The Act defines “key resources” as “publicly or privately controlled resources essential to the minimal operations of the economy and government.”