DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

JUL 2 2 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 08-007 – DoD Force Protection Threat Information

References: (a) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," November 7, 1982
(b) Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
(c) Deputy Secretary of Defense Memorandum, "Implementation of Interim Threat Reporting Procedures," September 13, 2007[1]
(d) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007

Purpose. This DTM establishes DoD policy and provides procedures for the documentation, storage, and exchange of force protection threat information related to the protection of DoD personnel, facilities, and forces in transit. This DTM is effective immediately; it shall be converted to a new DoD Directive within 180 days.

Applicability. This DTM applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

Policy. See Attachment 1 for DoD policy on force protection threat information.

Procedures. See Attachment 2 for procedures for reporting suspicious activity.

[1] Copies of this memorandum can be obtained from the Executive Services Directorate, Correspondence Control Division, Files Office at (703) 695-9717

Definitions. See section 1 of Attachment 2 for a definition of "suspicious activity" and Attachment 3 for a glossary of the categories of suspicious activity.

Releasability. This DTM is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

Gordon England
Deputy Secretary of Defense

Attachments:
As stated

ATTACHMENT 1

POLICY ON FORCE PROTECTION THREAT INFORMATION

1. It is DoD policy that:

a. The terrorist threat remains one of our Nation's most pervasive challenges. History has shown that DoD personnel, facilities, and activities make high-value terrorist targets, and no change is predicted for the future.

b. Force protection threat information guides DoD efforts to:

(1) Identify threats to the Department of Defense at the earliest opportunity.

(2) Implement information-driven and risk-based detection, prevention, deterrence, response, and protection efforts immediately.

(3) Identify persons involved in terrorism-related activities and long-term threats to the Department of Defense.

c. To strengthen DoD efforts to fight the terrorist threat:

(1) Those responsible for protecting DoD resources must have timely access to force protection threat information, particularly information that indicates a potential threat regarding those who want to attack us, their plans and activities, and the targets that they intend to attack.

(2) Force protection threat information shall be immediately available to, administered by, and shared among appropriate DoD law enforcement, force protection, antiterrorism, and security personnel in support of DoD missions.

(3) In addition, this information will be made available to other DoD Components to the maximum extent permitted by law, executive order, and directives for force protection purposes.

d. The DoD Components and sub-components shall document, store, and exchange personally-identifiable information concerning U.S. persons, in strict conformance with Federal law and DoD regulations. The sharing of this information, although critical to the success of the U.S. Government's terrorist-related efforts, must comply with all existing laws and regulations safeguarding personal freedoms, civil liberties, and information privacy.

2. This policy does not affect existing policies governing:

a. DoD Intelligence Component activities. DoD Intelligence Components may collect, retain, and disseminate information concerning U.S. persons pursuant to procedures set forth in DoD 5240.1-R Reference (a).

b. DoD Component acquisition of information concerning non-DoD personnel and organizations and the sharing of terrorism information in accordance with Executive Order 13388 Reference (b).

ATTACHMENT 2

PROCEDURES FOR REPORTING SUSPICIOUS ACTIVITY

1. IDENTIFYING SUSPICIOUS ACTIVITY. Suspicious activity is any behavior that is indicative of criminal activities, intelligence gathering, or other pre-operational planning related to a security threat to DoD interests worldwide. Although it is often difficult to determine whether a local incident has a terrorist nexus, similar incidents across many local jurisdictions may indicate the existence of a national threat.

2. REPORTING SUSPICIOUS ACTIVITY. The DoD Components shall:

a. Conduct suspicious activity reporting in accordance with the procedures in Deputy Secretary of Defense Memorandum Reference (c). These procedures shall remain in effect until the Department of Defense approves and implements a permanent force protection threat reporting system.

b. Submit to Defense Criminal Investigative Organizations and other DoD law enforcement or security authorities un-vetted Suspicious Activity Reports and other DoD non-intelligence reports dealing with information regarding a potential threat or suspicious activity, such as those listed in Attachment 3, that is related to DoD personnel, facilities, or forces in transit. The DoD Components shall share these reports with Combatant Command force protection and antiterrorism personnel.

c. NOT report information related to a U.S. person's ethnicity, race, religion, or lawful exercise of rights guaranteed by the Constitution or Federal law unless reasonable grounds exist that show a direct relationship of such information to a specific criminal act or behavior that may pose a threat to DoD personnel, facilities, and forces in transit.

d. In compliance with DoD Directive 5400.11 Reference (d):

(1) Establish rules of conduct for all persons involved in the design, development, operation, and maintenance of all threat reporting systems and associated processes.

(2) Train these persons with respect to these rules.

(3) Protect the rights of U.S. persons by ensuring personal information is not disseminated or disclosed to anyone who does not have the right and need to access such information.

e. Ensure subordinate organizations comply with these procedures and the policy in this DTM.

ATTACHMENT 3

GLOSSARY OF CATEGORIES OF SUSPICIOUS ACTIVITY

These terms and their definitions are for the purposes of this DTM.

acquisition of expertise. Unjustified attempts to obtain or conduct specialized training in security concepts, military weapons or tactics, or other unusual capabilities such as specialized transport or handling capabilities.

breach or attempted intrusion. Unauthorized entry or attempted entry into a restricted area or protected site; impersonation of authorized personnel (e.g., police, security, or janitorial personnel).

eliciting information for an unlawful purpose. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures at the facility or infrastructure.

expressed or implied threat. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.

flyover and/or landing. Suspicious overflight of and/or landing near a DoD facility or infrastructure by any type of flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, hang glider).

materials acquisition and/or storage. Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, and timers); unauthorized or unlicensed individual or group attempts to obtain precursor chemicals, agents, or toxic materials; and/or rental of storage units for the purpose of storing precursor material, chemicals, or apparatuses for mixing chemicals.

misrepresentation. Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

recruiting. Building operations teams and contacts, personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

sabotage, tampering, and/or vandalism. Damaging, manipulating, or defacing part of a DoD facility, infrastructure, or protected site.

surveillance. Monitoring the activity of DoD personnel, facilities, processes, or systems including showing unusual interest in a facility, infrastructure, or personnel (e.g., observation through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

testing of security. Interactions with or challenges to DoD installations, vessels, personnel, or systems that could reveal physical, personnel, or cyber security capabilities including attempts to compromise or disrupt DoD information technology infrastructures.

theft, loss, and/or diversion. Theft or loss associated with a DoD facility or infrastructure (e.g., of badges, uniforms, identification cards, emergency vehicles, technology, or documents whether classified or unclassified) that are proprietary to the facility, and/or a diversion of attention from a DoD facility or infrastructure that is related to a theft or loss associated with that facility.

weapons discovery. Discovery of weapons or explosives.