

OFFICE OF OPERATIONS COORDINATION: DHS OPERATIONAL REPORTING REQUIREMENTS

I. Purpose

This Directive establishes the Department of Homeland Security's (DHS) operational reporting requirements for events that fall outside the scope of the National Response Plan (NRP). This Directive and accompanying guide are the principal documents for leading, governing, integrating, and managing the situational awareness and reporting throughout DHS operational Components. This Directive also shifts the reporting mechanism to the DHS Homeland Security Information Network (HSIN).

II. Scope

A. This Directive applies to U.S. Citizenship and Immigration Services (USCIS), U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), Domestic Nuclear Detection Office (DNDO), U.S. Immigration and Customs Enforcement (ICE), U.S. Secret Service (USSS), Transportation Security Administration (TSA) and U.S. Visitor and Immigrant Status Indicator Technology Program Office (US-VISIT). This Directive applies to daily operational reporting, operational spot reports, and sensitive law enforcement actions/investigations.

B. This Directive does not apply to incident management/response events covered under the NRP.

III. Authorities

A. Public Law 107-296, "Homeland Security Act of 2002"

B. Secretary of Homeland Security Memorandum, dated September 12, 2003; Subject: DHS Leadership Meeting - Organizational Integration

C. President's Management Agenda, Fiscal Year 2002

IV. Policy and Requirements

This section provides the policy and requirements for DHS operational reporting. The OPS will rely on the reports identified in Instruction 252-06-001 to develop operational summaries for inclusion in the SMB and to provide situational awareness.

A. **Information Sharing Caveats:**

Components should include appropriate dissemination restrictions at the top and bottom of each report identified in Instruction 252-06-001, Part V.A (e.g., “FOR OFFICIAL USE ONLY”). The material may be further marked with the particular type of information being conveyed, e.g., “LAW ENFORCEMENT SENSITIVE,” “INTERNAL DHS USE ONLY,” etc.¹

B. **Geographic References:**

Each report identified in Instruction 252-06-001 will contain a geographic reference to the location(s) of the reported event. In order of preference, the geographic reference will include any one of the following:

- i. Either the name of the U.S. port-of-entry, airport, or a street address (including city and State);
- ii. Intersection, city, and State;
- iii. GPS coordinates; or
- iv. Compass directions in relation to an established point of land or facility, e.g., 3 miles NE of the San Ysidro Port-of-Entry, 2 nautical miles south of Key West, etc.

In the case of an individual or conveyance detained/stopped en route to another location, the Component will include both the geographic reference to the encounter location and the intended destination (i.e., the pre-encounter intended destination).²

¹ Components shall handle and transmit reports containing FOUO information in a manner authorized for FOUO transmission. See DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information (January 6, 2005).

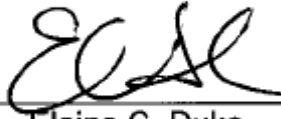
² For example, in the case of an alien Terrorist Identities Datamart Environment (TIDE) match who arrived at Boston Logan Airport from Paris, the Component would provide the encounter site (Boston Logan Airport) and the U.S. street address the traveler intended to visit.

C. **Media Releases:**

Components must notify OPS of any operational event described in DHS Instruction 252-06-001, Attachment 1, including accompanying photographs, if any, concurrently with or before issuing any media release.³

V. Questions

Address any questions or concerns regarding this Directive to the DHS Office of Operations Coordination, Current Operations Division.



Elaine C. Duke

Deputy Under Secretary for Management

2/12/08

Date

³ Components shall handle and transmit FOUO information in a manner authorized for FOUO transmission. See DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information (January 6, 2005). Components shall handle and transmit classified information in a manner authorized for classified transmission. See DHS Management Directive 11047, Protection of Classified National Security Information Transmission & Transportation (June 3, 2005).