ISE-AM-300

INFORMATION SHARING ENVIRONMENT ADMINISTRATIVE MEMORANDA (ISE-AM)

COMMON TERRORISM INFORMATION SHARING STANDARDS (CTISS) PROGRAM

1. Authority. The National Security Act of 1947, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; The 9/11 Commission Act of 2007; Presidential Memorandum dated April 10, 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); DNI memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388, and other applicable provisions of law.

2. Purpose. This issuance sets forth roles and responsibilities for the administration and implementation of Common Terrorism Information Sharing Standards (CTISS) issued by the PM-ISE.

3. Applicability. This ISE Administrative Memoranda (ISE-AM) is applicable to all Federal elements of the ISE, including the Office of the Program Manager, ISE (PM-ISE); the Information Sharing Council (ISC) members and their departments and agencies; and departments or agencies that possess or use terrorism-related information, operate a system that supports or interfaces to the ISE, or otherwise participate (or expect to participate) in the ISE, consistent with Section 1016(i) of the IRTPA, as amended. CTISS recommendations for non-Federal Government agencies will be published and provided by the PM-ISE, through the Attorney General and the Secretary of Homeland Security, for use by State, local, and tribal (SLT) governments, law enforcement agencies, and the private sector.

4. References. Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); *ISE Implementation Plan*, November 2006; *ISE Enterprise Architecture Framework (EAF)*, August 2007; *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment*, Version 1.0, September 2007; National Information Exchange Model, *Concept of Operations*, Version 0.5, January 9, 2007; Office of Director of National Intelligence Chief Information Officer, *Intelligence Community Enterprise Architecture Data Strategy*, August 2007 (Draft version); Office of Management and Budget (OMB), *Federal Transition Framework Catalog of Cross Agency Initiatives*, Version 1.0, December 2006; 28 Code of Federal Regulations (CFR) Part 23; OMB Circular A-119 (Transmittal Memorandum, Federal Participation in the Development and Use of Voluntary Standards; *CTISS Program Manual*, Version 1.0, October 2007.

5. Definitions.

a. *Common Terrorism Information Sharing Standards (CTISS)*: Business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. Two categories of common standards are formally identified under CTISS: functional standards and technical standards.

b. *Functional standards*: Rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas. Functional standards may be Government-unique or may be a combination of other functional standards as appropriate.

c. *Government-unique standards*: Standards developed by the Government for its own uses (OMB Circular A-119).

d. *Information resources*: Information and related resources, such as personnel, equipment, funds, and information technology (44 U.S.C. 3502(6)).

e. *Technical standards*: Specific technical methodologies and practices to design and implement information sharing capability into ISE systems.

f. *Voluntary consensus standards*: Standards developed or adopted by voluntary consensus standards bodies, both domestic and international (OMB Circular A-119).

6. Responsibilities.

a. The PM-ISE shall:

(1) Maintain and administer the CTISS program. Review and deconflict, as required, with other common standards programs used across the Federal Government.

(2) Select and issue the CTISS to all ISE participants under the ISE Issuance System.

(3) Ensure compatibility of the CTISS program with the ISE architecture program including those associated publications such as the ISE EAF and the Federal Enterprise Architecture (FEA)-ISE Profile.

(4) Integrate CTISS issuances into ISE budget guidance processes and performance metrics.

(5) Work with agencies to review cost impacts on existing and planned investments, documenting these potential impacts during standards selection and or development.

(6) Coordinate, publish, and monitor the CTISS program through the ISE Issuance System, as appropriate, including working with Federal agencies affected by the ISE that may not otherwise be represented by the ISC or foreign and private sector partners. Coordinate with the White House Office of Science and Technology Policy and with the National Institute of Standards and Technology (in the Department of Commerce) for formal nationwide publishing of the CTISS. Coordinate with the Attorney General and the Secretary of Homeland Security to share CTISS with state, local, and tribal (SLT) governments, law enforcement agencies, and the private sector.

(7) Designate a Chairperson for the CTISS Committee, under the ISC, with representatives from the following organizations:

a) ISC member departments and agencies;

b) Office of Management and Budget (E-Gov);

c) National Institute of Standards and Technology (NIST);

d) National Communications System (NCS);

e) Committee on National Security Systems (CNSS); and

f) State, Local, and Tribal Subcommittee of the ISC.

b. Each ISC member and other affected department or agency shall:

(1) Follow and incorporate guidance from the CTISS program and this issuance into its mission processes and supporting information resource planning and implementation as part of its participation in the ISE.

(2) Provide updates to the PM-ISE, as requested, on the implementation of the CTISS.

(3) Identify any implementation cost impacts on existing and planned investments and other potential impacts with CTISS initiatives.

(4) Provide assistance and recommendations to non-Federal ISE stakeholders associated with their department or agency on the implementation of the CTISS, as appropriate.

c. The CTISS Committee, established consistent with Section 1016(g)(4) of the IRTPA, shall:

(1) Identify and recommend functional standards and technical standards for issuance by the PM-ISE.

(2) Evaluate impacts and resolve potential incompatibility issues between CTISS and other standards programs in the Federal Government, SLT partners, and the private sector.

(3) Monitor CTISS implementation, under the authority of the ISC, and provide reports to PM-ISE, ISE agencies and OMB, as appropriate and requested.

7. Effective Date and Expiration. This ISE-AM is effective immediately and will remain in effect until superseded or cancelled.

Program Manager for the
Information Sharing Environment

Date: 31 OCT 2007