INFORMATION SHARING ENVIRONMENT GUIDANCE (ISE-G)

TECHNICAL STANDARD – CORE TRANSPORT

VERSION 1.0

1. <u>Authority.</u> The National Security Act of 1947, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; 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); Director of National Intelligence (DNI) memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law.

2. <u>Purpose.</u> This issuance serves as one piece of the initial suite of technical standards under the *Common Terrorism Information Sharing Standards (CTISS)* program for implementing information technology capabilities in the Information Sharing Environment (ISE) Core for Transport services. ISE Core Transport involves the underlying telecommunications and information technology infrastructures in the ISE Core which move information from one ISE Shared Space to another ISE Shared Space, to include email messages which may contain Sensitive But Unclassified (SBU) content.

3. <u>Applicability.</u> This ISE technical standard applies to all departments or agencies that possess or use terrorism, homeland security, or weapons of mass destruction information related to terrorism, operate systems that support or interface with the ISE, or otherwise participate (or expect to participate) in the ISE, consistent with Section 1016(i) of the IRTPA.

4. <u>References.</u> *ISE Implementation Plan*, November 2006; *ISE Enterprise Architecture Framework (EAF)*, August 2007; *ISE-AM-300: Common Terrorism Information Standards Program*, 31 October 2007; *Common Terrorism Information Sharing Standards Program Manual*, Version 1.0, October 2007; *National Strategy for Information Sharing*, October 2007; *ISE Profile and Architecture Implementation Strategy*, Version 1.0, May 2008; National Information Exchange Model, *Concept of Operations*, Version 0.5, January 9, 2007; 28 Code of Federal Regulations (CFR) Part 23.

5. <u>Definitions.</u>

    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. Functional standards set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas. Technical standards document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.
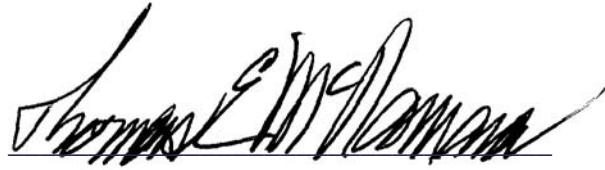
b. *Government-unique standards*: Standards developed by the Government for its own uses (OMB Circular A-119).

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

d. *ISE Core:* The ISE Core is the infrastructure made up of enterprise services, networks and systems that interconnect the individual ISE Shared Spaces into a functioning unified network. ISE Core exists within three information security domains (i.e., Top Secret/Sensitive Compartmented Information (SCI), Secret/Collateral, and Controlled Unclassified Information (CUI).

e. *ISE Shared Space:* The ISE Shared Spaces are where information is shared based upon clearly identified ISE-level mission need for such information and commonly agreed to business processes and information flows. ISE Shared Spaces and ISE Core allow ISE participants to leverage, for information-sharing purposes, their technologies and processes that are tightly coupled to their missions to support the larger national counterterrorism (CT) mission.

f. *National Information Exchange Model (NIEM):* A joint technical and functional standards program initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) that supports national-level interoperable information sharing.

g. *Universal Core (UCore):* An interagency information exchange specification and implementation profile. It provides a messaging framework for sharing the most commonly used data concepts of "who, what, when, and where". It serves as a starting point for data level integration and permits the development of richer domain specific exchanges. It was created and is managed by DOD, DOJ, DHS and the Intelligence Community.

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

6. <u>Guidance.</u> This ISE technical standard is hereby established for implementing information technology capabilities in the ISE Core for Transport services. ISE participants shall also ensure alignment of these technical standards with existing information technology standards for interfacing their ISE Shared Space to the ISE Core. It is based on current voluntary consensus standards for information technology resources used by the Federal Government, State/Local/Tribal (SLT) organizations, the private sector, and foreign partners, as appropriate.

7. Responsibilities.

    a. The Program Manager – ISE (PM-ISE), in consultation with the Information Sharing Council (ISC), shall:

        (1)   Maintain and administer this ISE technical standard.

        (2)   Publish and maintain configuration management of this ISE technical standard.

        (3)   Assist with the development of ISE Core Transport implementation guidance and governance structure, as appropriate, to address privacy, policy, architecture, and legal issues.

        (4)   Work with ISE participants, through the CTISS Committee, to develop a new or modified ISE technical standard, as needed.

        (5)   Coordinate, publish, and monitor implementation and use of this ISE technical standard, and coordinate with the White House Office of Science and Technology Policy, DNI Office of the Chief Information Office, and with the National Institute of Standards and Technology (in the Department of Commerce) for broader publication, as appropriate.

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

        (1)   Propose updates to the PM-ISE for this ISE technical standard, as appropriate.

        (2)   As appropriate, incorporate this ISE technical standard, and any subsequent implementation guidance, into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g., operations and maintenance {O&M} or enhancements).

        (3)   As appropriate, incorporate this ISE technical standard, and any subsequent implementation guidance, into budget activities associated with future or new development efforts for relevant mission specific programs, systems, or initiatives (e.g., development, modernization, or enhancement {DME}).

8. <u>Effective Date and Expiration.</u> This ISE-G is effective immediately and will remain in effect as the initial technical standard for ISE Core Transport until updated, superseded, or cancelled.

Thomas E. McNamara
Program Manager for the
Information Sharing Environment

Date: October 16, 2008

Attachment:
<u>Part A – ISE Technical Standards – Core Transport</u>

PART A – ISE TECHNICAL STANDARDS – CORE TRANSPORT

SECTION I – CORE TRANSPORT

The following constitutes those technical voluntary consensus standards to be followed primarily by ISE Core Implementation Agents in planning, implementing, and providing Core infrastructure to the ISE. ISE participants shall also ensure alignment of these technical standards with existing information technology standards for interfacing their ISE Shared Space to the ISE Core. The tables below provide the core transport technical standards identified for use within the ISE Core. The tables list the standards by Open System Interconnection (OSI) layers (Transport, Network, Link, Physical, and Application), standard (Standard), implementing authoritative body (Standards Body), and a brief description (Standards Description).

Table 1 – Core OSI Transport Layer Technical Standards

OSI Layer	Standard	Standards Body	Standards Description
Transport	Transmission Control Protocol (TCP)	IETF	*Provides reliable, in-order delivery of a stream of bytes, providing application suitability. (Basic)*
	User Datagram Protocol (UDP)	IETF	*Core protocol of the Internet Protocol suite that allows networked computers to send short messages sometimes known as datagrams (using Datagram Sockets) to one another. (Basic)*

Table 2 – Core OSI Network Layer Technical Standards

OSI Layer	Standard	Standards Body	Standards Description / Version / Date
Network	Internet Group Management Protocol (IGMP)	IETF	Protocol used by IPv4 systems (hosts and routers) to report IP multicast group memberships to neighboring multicast routers. Version 3, dated Oct 2002.
	Ping (PING)	IETF	Computer network tool used to test whether a host is reachable across an IP network; also used to self test network interface card of the computer. (Basic)
	Distance Vector Multicast Router Protocol (DVMRP)	IETF	Interior gateway protocol; suitable for use within an autonomous system, but not between different autonomous systems. (Basic)
	Enhanced Interior Gateway Routing Protocol (EIGRP)	IETF	Advanced distance-vector routing protocol, with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router. (Basic)
	Intrazone Routing Protocol (IARP)	IETF	Protocol that proactively tracks local network connectivity; provides support for route acquisition and route maintenance. (Basic)
	Internet Control Message Protocol (ICMP)	IETF	Protocol used for host-to-host datagram service in a system of interconnected networks. (Basic)
	Interzone Routing Protocol (IERP)	IETF	Reactive routing protocol that tries to find a route only on demand. (Basic)
	Interior Gateway Routing Protocol (IGRP)	IETF	Protocol that provides robust routing within an autonomous system. (Basic)
	Internet Protocol Version 4 (IPv4)	IETF	Data-oriented protocol to be used on packet switched internetworks; best effort protocol, does not guarantee delivery. (Basic)
	Internet Protocol Version 6 (IPv6)	IETF	Network layer for packet-switched internetworks; much larger address space, allowing greater flexibility in assigning addresses. (Basic)
	Intermediate System to Intermediate System (IS-IS)	ITU	Protocol used by network devices (routers) to determine the best way to forward datagrams or packets through a packet-based network. (Basic)
	Open Shortest Path First (OSPF)	IETF	Hierarchical interior gateway protocol (IGP) for routing in Internet Protocol; used to calculate the shortest path tree inside each area. Version 3, dated 1999 (supports IPv6). Version 2, dated 1998 (supports IPv4).
	Protocol Independent Multicast - Sparse Mode (PIM-SM)	IETF	Protocol for efficiently routing to multicast groups that may span wide-area (WAN and inter-domain) internets. (Basic)
	Protocol Independent Multicast - Dense Mode (PIM-DM)	IETF	Primarily designed for routing to multicast LAN applications.(Basic)
	Dynamic Host Configuration Protocol (DHCP)	IETF	Protocol used by networked devices to obtain various parameters necessary to operate in an Internet Protocol (IP) network. (Basic)
	X.25 Layer 3	ITU	Used for packet switch data communication. (Basic)
	X.75 Layer 3	ITU	Defines interconnections between multiple X.25 networks. (Basic)

Table 3 – Core OSI Link Layer Technical Standards

OSI Layer	Standard	Standards Body	Standards Description / Version / Date
Link	Asynchronous Transfer Mode (ATM)	ITU	Cell relay, packet switching network, and data link layer protocol that encodes data traffic into small fixed-sized cells. (Basic)
	Ethernet	IEEE	Family of frame-based computer networking technologies for LANs. (Basic)
	Frame Relay	ITU	Efficient data transmission technique used to send digital information quickly and cheaply in a relay of frames to one or many destinations from one or many end-points. (Basic)
	Label Distribution Protocol (LDP)	IETF	Protocol that defines a set of procedures and messages by which one LSR informs another of the label bindings it has made. (Basic)
	Link Layer Discovery Protocol (LLDP)	IEEE	Vendor-neutral Layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network, dated May 2005. (Basic)
	LLDP - Media Endpoint Discovery	TIA	Protocol used to communicate between switch ports and endpoint devices, dated 2006. (Basic)
	Multiprotocol Label Switching (MPLS)	IETF	Provides unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model; can be used to carry many different kinds of traffic. (Basic)
	Point-to-Point Protocol (PPP)	IETF	Protocol for connection over synchronous and asynchronous circuits; designed to work with numerous network layer protocols. (Basic)
	Point-to-Point Tunneling Protocol (PPTP)	IETF	Protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating VPN across TCP/IP-based data networks. (Basic)
	Serial Line Internet Protocol (SLIP)	IETF	Protocol used for communication between two machines that are previously configured for communication with each other. Modifies standard Internet datagram by appending a special "SLIP END" character to it; allows datagrams to be distinguished as separate. (Basic)
	Spanning Tree Protocol (STP)	IEEE	Protocol that ensures a loop-free topology for any bridged LAN. (Basic)
	X.25 Layer 2	ITU	Used for packet switch data communication. (Basic)
	X.75 Layer 2	ITU	Defines the interconnection of two X.25 networks. (Basic)

Table 4 – Core OSI Physical Layer Technical Standards

OSI Layer	Standard	Standards Body	Standards Description / Version / Date
Physical	Generalized Multiprotocol Label Switching (GMPLS)	ITU	Enhances MPLS architecture by completely separating the control and data planes of various networking layers; enables a seamless interconnection and convergence of new and legacy networks. (Basic)
	Integrated Services Digital Network (ISDN)	ITU	Allows digital transmission of voice and data over ordinary telephone copper wires; typically provides a maximum of 128 kbit/s. (Basic)
	Plesiochronous Digital Hierarchy (PDH)	ITU	Technology used in telecommunications networks to transport large quantities of data over digital transport equipment. (Basic)
	RS-232	EIA	Standard which defines communication between a DTE (Data terminal equipment) and a DCE (Data Circuit-terminating Equipment). (Basic)
	RS-422	EIA	Provides for data transmission, using balanced or differential signaling, with unidirectional/non-reversible, terminated or non-terminated transmission lines, point to point, or multi-drop. (Basic)
	RS-485	EIA	Widely used communication interface in data acquisition and control applications where multiple nodes communicate with each other. (Basic)
	Synchronous Digital Hierarchy (SDH)	ITU	Standard technology for synchronous data transmission on optical media. (Basic)
	Synchronous Optical Network (SONET)	ITU	Network technology designed to carry large volumes of traffic over relatively long distances on fiber optic cabling. (Basic)

Table 5 – Core OSI Application Layer Technical Standards

OSI Layer	Standard	Standards Body	Standards Description / Version / Date
Application	Border Gateway Protocol (BGP)	IETF	Exchanges network reachability information with other BGP systems. (Basic)
	Real-Time Transport Protocol (RTP)	IETF	Protocol that provides end-to-end delivery services for data with real-time characteristics. (Basic)
	Real-Time Transport Control Protocol (RTCP)	IETF	Protocol that provides control for an RTP session. Particularly, it allows devices to exchange information about the quality of the media session, including such information as jitter, packet loss, and a host of other statistics. (Basic)
	Simple Network Management Protocol (SNMP)	IETF	Network management specification that provides standard, simplified, and extensible management of LAN-based internetworking products. (Basic)
	Secure Sockets Layer (SSL)	IETF	Provides privacy and reliability between two communicating applications. (version 0.9.8i, dated Sept 2008)
	Transport Layer Security (TLS)	IETF	Provides privacy and data integrity between two communicating applications. (Basic)
	Simple Object Access Protocol (SOAP)	W3C	Protocol intended for exchanging structured information in a decentralized, distributed environment. Version 1.1, dated April 2007. (Basic)