

---

## INFORMATION SHARING ENVIRONMENT GUIDANCE (ISE-G)

### TECHNICAL STANDARD – INFORMATION ASSURANCE

#### VERSION 1.0

---

1. Authority. The National Security Act of 1947, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated 10 April 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated 16 December 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); Director of National Intelligence (DNI) memorandum dated 2 May 2007 (Program Manager’s Responsibilities); Executive Order 13388; and other applicable provisions of law.
2. Purpose. 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) for Information Assurance (IA) services. The governance and risk management processes for the ISE are critical to establishing and maintaining effective IA for the ISE. The artifacts of governance arrangements and activities are policies, rules, guidelines, recommendations for changing laws, and decision making that affect all aspects of the ISE, including establishing and maintaining a known and acceptable level of risk for the ISE. IA is a key capability in the ISE to support business process-driven exchanges.
3. Applicability. This ISE technical standard applies to all departments or agencies that possess or use information related to terrorism, homeland security, or weapons of mass destruction 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 IRPTA. Information obtained by activities conducted pursuant to sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947 is excluded.
4. References. *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, 9 January 2007; 28 Code of Federal Regulations (CFR) Part 23.

## 5. Definitions.

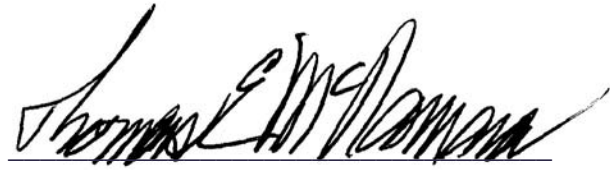
- a. *Common Terrorism Information Sharing Standards (CTISS)*: Business process-driven, performance-based “common standards” for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. Two categories of common standards are formally identified under CTISS: functional standards and technical standards. 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: Top Secret/Sensitive Compartmented Information (SCI), Secret/Collateral, and Controlled Unclassified Information (CUI)/Sensitive but Unclassified (SBU).
- e. *ISE Shared Spaces*: The ISE Shared Spaces are where information is shared based upon clearly identified ISE-level mission needs for such information and commonly agreed-to business processes and information flows. ISE Shared Spaces and the 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. Guidance. This ISE technical standard is hereby established for implementing information technology capabilities in the ISE Core for IA 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 IA 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 Officer, 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. Effective Date and Expiration. This ISE-G is effective immediately and will remain in effect as the initial technical standard for ISE IA until updated, superseded, or cancelled.

A handwritten signature in black ink, appearing to read "Thomas E. McNamara", written over a horizontal line.

Thomas E. McNamara  
Program Manager for the  
Information Sharing Environment

Date: October 24, 2008

Attachment:

Part A – ISE Technical Standards – Information Assurance

## PART A – ISE TECHNICAL STANDARDS – INFORMATION ASSURANCE

### SECTION I – INFORMATION ASSURANCE

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. These standards are not intended to be all inclusive; however, they are provided as a baseline of standards to be used by ISE participants within the ISE Core. 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. Table 1 below provides the Information Assurance standards (Standard) identified for use within the ISE Core, the implementing authoritative organization (Standards Body), and a brief description of the standard and the version and date of latest release of the standard (Standards Description/Version/Date).

*Table 1 – Information Assurance Technical Standards*

Standard	Standards Body	Standards Description / Version / Date
X.509 Authentication framework	ITU-T	Standard certificate format for public key certificates and certification validation. Version 3, dated Mar 2000.
FIPS 140-2 Security Requirements for Cryptographic Modules	NIST	Standard specifies security requirements that will be satisfied by a cryptographic module used within a security system protecting sensitive but unclassified information, dated Dec 2002.
FIPS 200 Minimum Security Requirements for Federal Information and Information Systems	NIST	Standard specifies minimum security requirements for Federal information and information systems in 17 security-related areas, dated Mar 2006
SP 800-57 Recommendation for Key Management	NIST	Provides cryptographic key management guidance, dated Mar 2007.
FIPS 197 Advanced Encryption Standard (AES)	NIST	Specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data, dated Nov 2001.
SP 800-21 Guideline for Implementing Cryptography in the Federal Government	NIST	Provides a structured, yet flexible set of guidelines for selecting, specifying, employing, and evaluating cryptographic protection mechanisms in Federal information systems, second edition dated Dec 2005.
FIPS 180-2 Secure Hash Algorithm	NIST	Specifies secure hash algorithms for computing a condensed representation of electronic data (message), dated Aug 2002.
FIPS 186-2 Digital Signature Standard	NIST	Specifies algorithms appropriate for applications requiring a digital, rather than written, signature, dated Jan 2000.
HAIPE National Policy Guidance	CNSS	Provides governance for the procurement of IP encryption products for Fiscal Year (FY) 2009 and beyond, dated Feb 2007.

Standard	Standards Body	Standards Description / Version / Date
IETF RFC 2104 – Keyed Hashing for Message Authentication	IETF	A mechanism for message authentication using cryptographic hash functions, dated February 1997
IETF RFC 2246 – Transport Layer Security (TLS) Protocol	IETF	Internet standards track for the Internet community, Version 1.0, dated Jan 1999
IETF RFC 2401 – Security Architecture for the Internet Protocol	IETF	Internet standards track for the Internet community, dated November 1998
IETF RFC 2402 – IP Authentication Header	IETF	Internet standards track protocol for the Internet community, dated November 1998
IETF RFC 2404 – Use of HMAC-SHA-1-96 Within ESP and AH	IETF	Internet standards track protocol for the Internet community, dated November 1998
IETF RFC 2406 – IP Encapsulating Security Payload	IETF	Internet standards track protocol for the Internet community, dated November 1998
IETF RFC 2407 – Internet IP Security Domain of Interpretation for ISAKMP Internet Draft	IETF	Internet standards track protocol for the Internet community, dated November 1998
IETF RFC 2408 – Internet Security Association and Key Management Protocol	IETF	Internet standards track protocol for the Internet community, dated November 1998
IETF RFC 2409 – Internet Key Exchange	IETF	Internet standards track protocol for the Internet community, dated November 1998
IETF RFC 2420 – PPP Triple-DES Encryption Protocol	IETF	Internet standards track protocol for the Internet community, dated September 1998
IETF RFC 2587 – Internet X.509 PKY LDAPv2 Schema	IETF	Internet standards track protocol for the Internet community, dated Jun 1998
IETF RFC 3845 – DNS Security NextSECure RDATA Format	IETF	Internet standards track protocol for the Internet community, dated August 2004
IETF RFC 2845 – Secret Key Transaction Authentication for DNS	IETF	Internet standards track protocol for the Internet community, dated May 2000
IETF RFC 3075 – Signature Syntax and Processing	IETF	Internet standards track protocol for the Internet community, dated Mar 2002
IETF RFC 4051 – Additional XML Security Uniform Resource Identifiers (URIs)	IETF	Internet standards tracking protocol for the Internet community, dated Apr 2005
IETF RFC 3852 – Cryptographic Message Syntax (CMS)	IETF	Internet standards track protocol for the Internet community, dated Apr 2007

Standard	Standards Body	Standards Description / Version / Date
RSA Labs PKCS#12:1999 – Personal Exchange Syntax Standard	RSA	Personal Information Exchange Syntax Standard, Version 1.0, RSA, dated 24 June 1999.
RSA Labs PKCS#15:1999 – Cryptographic Token Information Format Standard	RSA	Cryptographic Token Information Format Standard, Version 1.1, RSA, dated 6 June 2000.
Extensible Configuration Checklist Description Format	NIST	Language for writing security checklists, benchmarks, and related kinds of documents, dated Jan 2008.
Open Vulnerability and Assessment Language (OVAL)	NIST	International, information security, community standard to promote open and publicly available security content and to standardize the transfer of this information across the entire spectrum of security tools and services. Version 5.5, dated Oct 2008.

Table 2 provides generic standards identified for use within the ISE Core, the implementing authoritative organization (Standards Body), and a brief description of the standard and the version and date of latest release of the standard (Standards Description/Version/Date).

**Table 2 – Generic ISE Technical Standards**

Standard	Standards Body	Standards Description / Version / Date
Extensible Markup Language (XML)	W3C	Flexible text format designed to meet the challenges of large-scale electronic publishing. Version 1.0, Fifth Edition, dated Feb 2008.
Standard Generalized Markup Language (SGML)	ISO 8879; W3C	International standard for the description of marked-up electronic text, dated 1986.
Security Assertion Markup Language (SAML)	OASIS	An XML standard that allows secure Web domains to exchange user authentication and authorization data. Version 2.0, dated Mar 2005.
XACML 2.0 eXtensible Access Control Markup Language	OASIS	Standard that describes both a policy language and an access control decision request/response language. Version 1.0, dated Feb 2003.
Extensible Stylesheet Language (XSL)	W3C	Language used to express stylesheets. Version 1.0, dated Oct 2001.
Extensible Stylesheet Language Transformations (XSLT)	W3C	Language that describes a way to locate and process XML documents by using an addressing syntax based on a path through the documents' logical structure. Version 1.0, dated Nov 1999.
XML Key Management Specification (XKMS 2.0)	W3C	Governs how to incorporate cryptography into a system. XKMS Version 2.0, dated Mar 2001.
XML Path Language (XPath)	W3C	Language for addressing parts of an XML document, designed to be used by both XSLT and XPointer. Version 1.0, dated Nov 1999.

Table 3 below provides a list of recommended guidance standards for participants in the ISE Core. It lists the issuance organization and a short description and release date of the recommended guidance standard. Where necessary, these guidance standards may be used by ISE participants as best-in-practice reference materials to develop policies within their respective environments.

**Table 3 – Recommended Guidance / Standards**

Standards Body / Organization	Recommended Standards Description / Version / Date
NIST	FIPS Pub 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i> , dated Feb 2004.
	FIPS Pub 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i> , dated Mar 2006.
	NIST SP 800-18, <i>Guide for Developing Security Plans for Federal Information Systems, Revision 1</i> , dated Feb 2006.
	NIST SP 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i> , dated May 2004.
	NIST SP 800-53, <i>Recommended Security Controls for Federal Information Systems, Rev 2</i> dated Dec 2007.
	NIST SP 800-53A, <i>Guide for Assessing the Security Controls in Federal Information Systems</i> , dated July 2008
	NIST SP 800-59, <i>Guideline for Identifying an Information Systems as a National Security System</i> , dated Aug 2003.
	NIST SP 800-60, <i>Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1</i> , dated Aug 2008.
	NIST SP 800-70, <i>Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers</i> , dated May 2005.
	NIST SP 800-100, <i>Information Security Handbook, A Guide for Managers</i> , dated Oct 2006.
ISO/IEC	ISO/IEC 27001:2005 – Specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS), dated Oct 2005.
	ISO/IEC 27002:2005 – Outlines potential controls and control mechanisms for an ISMS, dated Jun 2005.
	ISO/IEC 24727 – Programming interfaces for interactions between integrated circuit cards and external applications, to include generic services for multi-sector use, dated Jan 2007.
CVE	Common Vulnerabilities and Exposures – a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities.
CCE	Common Configuration Enumeration (CCE) – provides identifiers for security configuration issues and exposures.
CPE	Common Platform Enumeration (CPE) – structured naming scheme for information technology systems, software, and packages.
CVSS	Common Vulnerability Scoring System (CVSS) – assesses the severity of computer system security vulnerabilities.
NSTISSI	National Information Assurance Certification and Accreditation (NIACAP) 1000 – process designed to certify that the information system (IS) meets documented security requirements and will continue to maintain the accredited security posture throughout the system life cycle, dated Apr 2000



Standards Body / Organization	Recommended Standards Description / Version / Date
DOD	Department of Defense Directive (DODD) 8500.1 – Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology and supports the evolution to network centric warfare, dated Nov 2003
	Department of Defense Instruction (DODI) 8500.2-H – Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks, dated Feb 2003