Co-Chairs of ANSI's JTC/CS1- ICT SCRM AdHoc Working Group:

Contribution to the NIST RFI on Developing a Framework To Improve Critical Infrastructure Cybersecurity.

Overview

The Co-Chairs of International Committee for Information Technology Systems (INCITS)/CyberSecurity 1 (CS1) Information Communication Technology (ICT) Supply Chain Risk Management (SCRM) Ad Hoc group are pleased to submit this response to NIST Request for Information (RFI) as an input into the development of Cybersecurity Framework. CS1 ICT SCRM Ad Hoc has established a successful model for targeted US government engagement in international standards development. In this response, the Co-chairs – Don Davidson of the Department of Defense Trusted Mission Systems and Networks (DoD TMSN) and Nadya Bartol of Utilities Telecom Council (UTC) – provide a brief summary of how the CS1 ICT SCRM Ad Hoc was established, its objectives, and its accomplishments.

Globalization has brought a unique set of Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) challenges and threats to governments, critical infrastructure and industry, especially with our ever-increasing reliance on ICT products and services to meet mission and business needs. This ICT globalization challenge spawned the US Comprehensive Initiative (#11) on Supply Chain Risk Management (CNCI-SCRM), which includes not only initiatives inside the US government, it also includes, pursuit of "commercially acceptable global sourcing standards". The overarching vision of this latter effort is for US and other governments to successfully cooperate with their national and multinational industry partners to identify and understand risks associated with a global ICT supply chain and to implement and mature practices to manage that risk. These practices should be based on commercial and international global sourcing standards that are well understood by all stakeholders, and then used to manage risks associated with globalized ICT. Establishing both national and international ICT SCRM stakeholder communities has been successful; a primary mechanism that enabled this success is the establishment of INCITS/CS1 ICT SCRM AdHoc Group. The ICT SCRM Ad Hoc is co-chaired by government and industry representatives. There have been over 100 participants in the group, with about 30 individuals participating in the ICT SCRM Ad Hoc on a regular basis, including numerous industry, academia, and government representatives.

The ICT SCRM challenge impacts every government and commercial organization that acquires ICT products and services. Furthermore, many of the suppliers of ICT products and services also find themselves facing these same ICT globalization challenges when they are acquiring ICT products and services to integrate into their own solutions and therefore have a broad interest in facing the ICT SCRM challenge.

ICT SCRM efforts include a wide variety of efforts, but are primarily focused on opportunities within ISO/IEC JTC 1 SC 27, The Open Group's Trusted Technology Forum (OTTF), "Common Criteria" and US ICT

SCRM guidance development by National Institute of Standards and Technology (NIST). (See Annex A for a Landscape of SCRM Standards Activities)

In the 1990's the US government moved away from their "customized" military-specifications & military-standards philosophy, to a more commercial based standards approach, however they did not accompany that policy change with an increased engagement capability/capacity with that commercial standards community. OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities. This Circular directs all federal agencies to use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical. The policies in this Circular are intended to reduce to a minimum the reliance by agencies on government-unique standards. (http://www.whitehouse.gov/omb/circulars_a119). The new "Ad Hoc Group Approach" is a useful representative/model example for targeting US engagement with Standards Development Organizations (SDO).

The success of several ICT SCRM Standards efforts is attributable to the collaborative efforts with the stakeholder community to identify processes, practices, and standards that can be of use, and to develop additional standards for those particular aspects of the problem that are currently not standardized. There are multiple standards activities across the spectrum of functional disciplines and works with the stakeholders identifying applicable best practices and including them in emerging standards.

ICT-SCRM Stakeholders participate in a number of ongoing industry efforts and groups in ICT SCRM and related best practice and standard creation. Best practices are developed and tested primarily by industry and can be adopted by a variety of stakeholders, including US and other governments.

Collaborating on Standards

In February 2009, CS1, which is chartered with representing US interested within the International Organization for Standardization committee (known as ISO/IEC JTC1 SC27) established ICT SCRM Ad Hoc Group to explore existing best practices and create a community of interest that could contribute meaningful technical content to a new standard. In November 2009, CS1 proposed to international community to develop a new standard to address ICT SCRM. After an initial study period, 10 other countries supported the creation of a new standard ISO/IEC 27036: Information technology – Security techniques – Information Security for Supplier Relationships. A number of national bodies and liaison organizations (Belgium, Canada, China, France, Japan, Korea, Luxembourg, Malaysia, Russia, Singapore, South Africa, Sweden, Switzerland, United Kingdom, US, Information Security Forum (ISF), ISACA) actively supported the effort and provided comments on each draft. The consolidated contributions from the technical experts participating in the CS1 ICT SCRM Ad Hoc provided a solid foundation for the US contribution and US positions. This ensured that as the content was technically sound, complete, and articulated with clarity. Since November 2010 when the standard was officially approved, ISO/IEC 27036, Parts 1, 2 and 3 have rapidly progressed to Draft International Standard (DIS) status. Recently, within CS1, a Cloud Ad Hoc and Storage Ad Hoc have been established, using the ICT SCRM Ad Hoc as a

model for reaching the technical expertise to provide a solid US position on these important emerging technical areas. The Co-chairs have been recognized by the INCITS Team award for their leadership and dedicated efforts that lead to the exceptional quality and timeliness of standards.

NOTE: A complementary ICT SCRM effort is led by the Open Group. The Open Group Trusted Technology Forum (OTTF) leads the development of a global supply chain integrity program and framework in order to provide buyers of IT products with a choice of accredited technology partners and vendors. The Open Group Trusted Technology Provider Standard (O-TTPS) will identify best practices for secure engineering and supply chain integrity that distinguish trusted technology providers, and foster a secure and sustainable global supply chain. The result of this effort is being considered for submission as a 5th part of ISO/IEC 27036. Additionally, OTTF and "new Common Criteria-protection profile" developments are working to harmonize their process accreditation and product certification efforts.

The ICT SCRM Ad Hoc model provided the US community of ICT SCRM stakeholders an opportunity to more effectively engage the international ICT SCRM community and successfully advocate US positions. The ICT-SCRM Ad Hoc is restricted to US based organizations. It meets approximately every two months, shares information on on-going ICT SCRM initiatives, and shapes US national positions on ICT SCRM related ISO/IEC, ISO, and IEC developments. Results of ICT SCRM AdHoc data collection, analysis and results are included at Annexes A-B-C.

Information Sharing Across Standards Community

From the people perspective, the stakeholder community works to ensure sharing of information including best practices, relevant standards, useful existing technologies, and potentially useful emerging technologies. Because of the multidisciplinary nature of ICT SCRM stakeholders may not be aware of potential solutions when these solutions are outside of stakeholders' functional discipline. Outreach aims to educate stakeholders across functional disciplines to facilitate identification of gaps, expand adoption of best practices and standards, and increase the use of existing or emerging technologies. Outreach activities include: development of awareness and education materials; collaborative work with various interagency, public-private, and industry groups; and presentations and panels at conferences of interest to stakeholders.

From the technology perspective, ICT SCRM stakeholders identify existing and emerging technologies and works to publicize them to other stakeholders through a variety of outreach activities. Stakeholders facilitate introduction of technologies into SDOs as appropriate.

Figure 1 demonstrates the process flow within ICT SCRM Standards Stakeholder community.

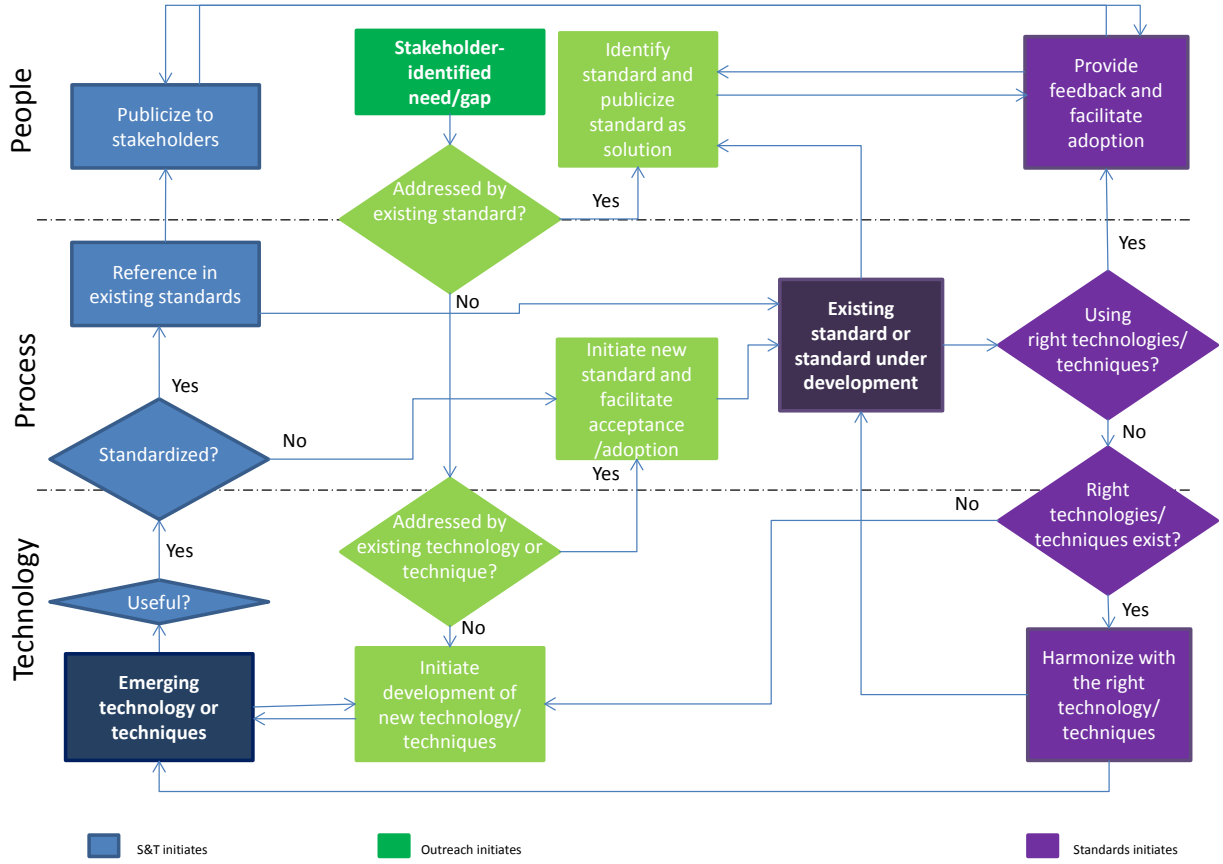

Figure 1. ICT SCRM Standards Program Process Flow

As an example of how these interdependencies have contributed to solving ICT SCRM challenge, stakeholder efforts through CS1 ICT SCRM Ad Hoc resulted in:

- Identification and collection of ICT SCRM best practices which were candidates for standardization
- Acceptance for the development of an ICT SCRM standard within the US
- Approval of ISO/IEC 27036, Information Technology – Security Techniques – Information Security for Supplier Relationships
- Addition of content to ISO/IEC 27001 and ISO/IEC 27002 that helps ensure inclusion of ICT SCRM as a consideration in information security management
- Addition of content to ISO/IEC 27034 which enhances ICT SCRM considerations in application security activities.

Standards Harmonization Example

Stakeholders understand that a variety of standards are needed to enable organizations to leverage the standards that best support the mitigation of enterprise specific risks. The use of consensus-based standards developed by industry, with the overall goal of raising the bar for the commercial global sourcing practices, provides the framework to address the ICT SCRM challenge. These standards should apply to broad stakeholder communities including DoD (.mil), Civil Agencies (.gov), and the industry (.com) and address a broad set of ICT SCRM-related topics including software and hardware assurance, counterfeits, and cloud computing. Figure 2 provides a snapshot of the relationship of existing standards that contribute to ICT SCRM.

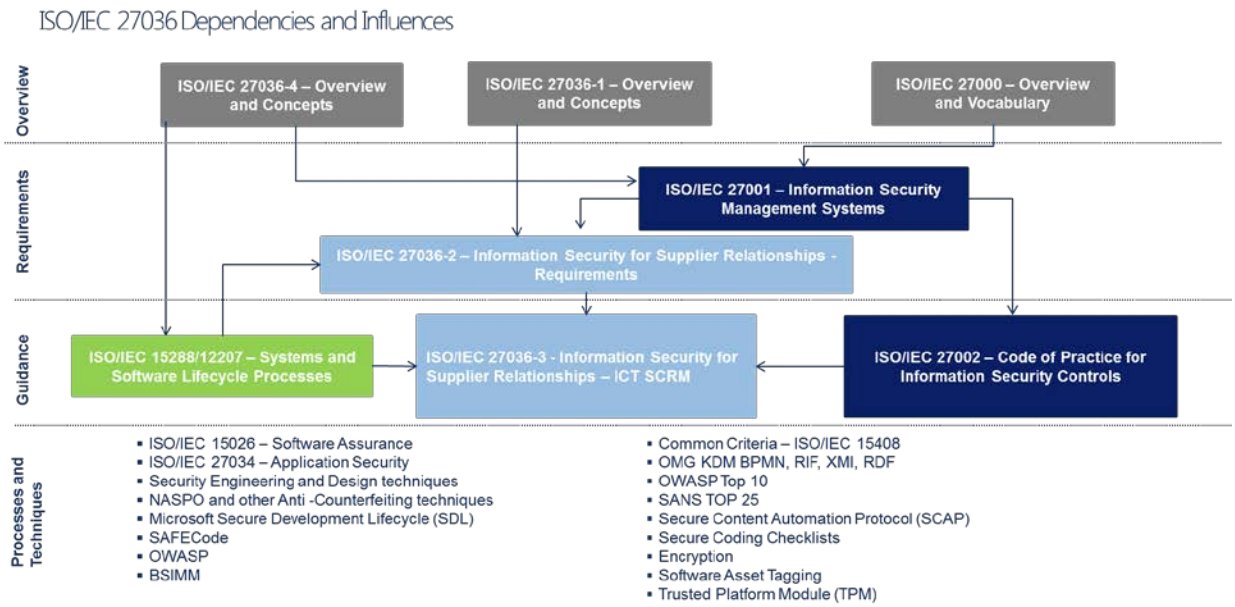

Figure 2. Standards Contributing to SCRM

SDO Engagement Model

ICT SCRM is a community effort with many concurrent initiatives and a multitude of stakeholders. To ensure appropriate level of engagement, Stakeholders prioritizes these initiatives (including emerging standards and technologies) as they become known to the organizations and each stakeholder engages in one of the following ways based on the relevance of the initiative to their organization goals:

- **Participate:** Act as an active participant in the development of standards surrounding the described topic
- **Influence:** Serve as a trusted advisor and consultant in the development of standards surrounding the described topic
- **Monitor:** Monitor the topic area for possible increased involvement.

Annex A: The Cybersecurity Standards Landscape

The study of ICT SCRM standards landscape was completed in January 2010 in the form of a document and a key graphic provided in Figure A-1.

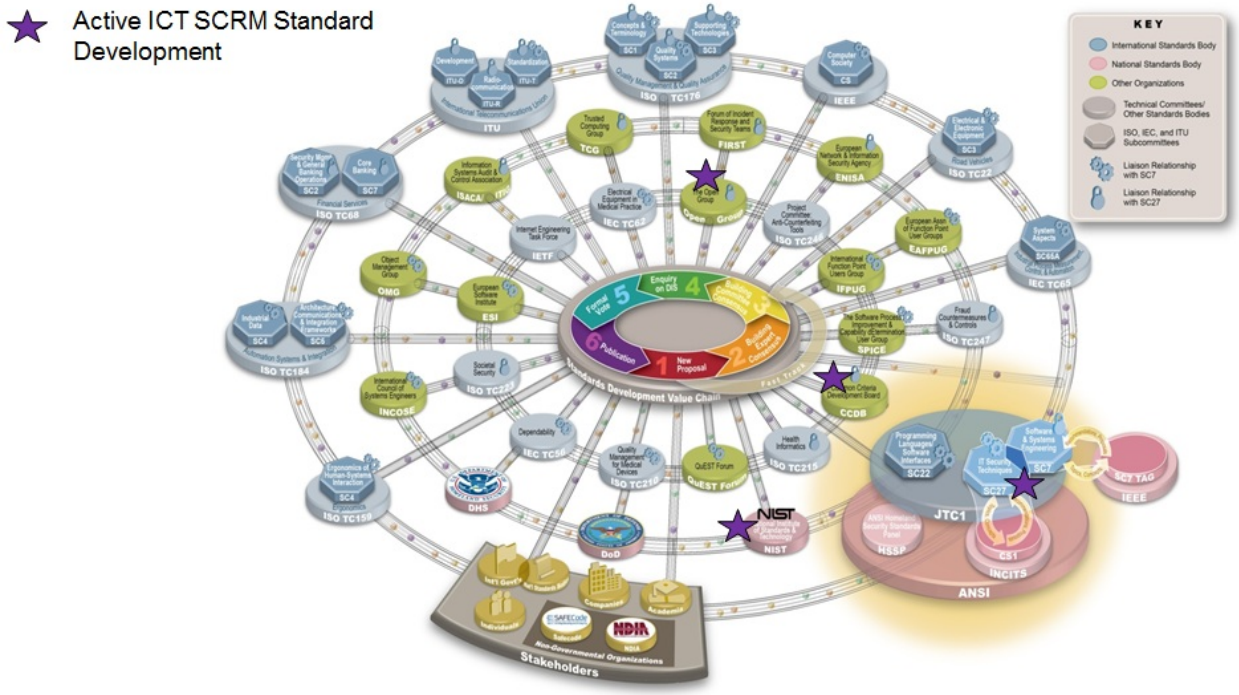

Figure A-1. ICT SCRM Standards Development

The graphic and the corresponding Standards Landscape document are based on the portfolio of two international committees under the auspices of ISO/IEC JTC1: SC 27 that focuses on IT Security Techniques; and SC7 that focuses on System and Software Engineering. The graphic is color-coded as follows:

- Blue indicates Standards Development Organization (SDO) groups associated with ISO, IEC, or ITU
- Green indicates other SDOs
- Pink indicates US-based organizations including the Technical Advisory Groups for SC7 (SC7 TAG) and SC27 (CS1), their parent organizations (IEEE and ANSI), as well as US

government agencies engaged in the development of ICT SCRM standards (NIST, DoD, DHS)

- Purple stars indicate specific SDOs currently engaging in the development of ICT SCRM content, both nationally and internationally, including SC27, SC7, The Open Group, Common Criteria Development Board (CCDB), and NIST. Note these same starred areas are where DoD chose to engage with their information sharing activities.

Annex B: Current Portfolio of SC27 Standards Efforts

- ISO/IEC 7064:2003 Information technology -- Security techniques -- Check character systems
- ISO/IEC 9796-2:2010 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
- ISO/IEC 9796-3:2006 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms
- ISO/IEC 9797-1:2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
- ISO/IEC 9797-2:2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
- ISO/IEC 9797-3:2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 3: Mechanisms using a universal hash-function
- ISO/IEC 9798-1:2010 Information technology -- Security techniques -- Entity authentication -- Part 1: General
- ISO/IEC 9798-2:2008 Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms
- ISO/IEC 9798-3:1998 Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques
- ISO/IEC 9798-4:1999 Information technology -- Security techniques -- Entity authentication -- Part 4: Mechanisms using a cryptographic check function
- ISO/IEC 9798-5:2009 Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero-knowledge techniques
- ISO/IEC 9798-6:2010 Information technology -- Security techniques -- Entity authentication -- Part 6: Mechanisms using manual data transfer
- ISO/IEC 10116:2006 Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
- ISO/IEC 10118-1:2000 Information technology -- Security techniques -- Hash-functions -- Part 1: General
- ISO/IEC 10118-2:2010 Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher
- ISO/IEC 10118-3:2004 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
- ISO/IEC 10118-3:2004/Amd 1:2006 Dedicated Hash-Function 8 (SHA-224)
- ISO/IEC 10118-4:1998 Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic
- ISO/IEC 11770-1:2010 Information technology -- Security techniques -- Key management -- Part 1: Framework
- ISO/IEC 11770-2:2008 Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
- ISO/IEC 11770-3:2008 Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques
- ISO/IEC CD 11770-3 Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques
- ISO/IEC 11770-4:2006 Information technology -- Security techniques -- Key management -- Part 4: Mechanisms based on weak secrets

- ISO/IEC 11770-5:2011 Information technology -- Security techniques -- Key management -- Part 5: Group key management
- ISO/IEC 11889-1:2009 Information technology -- Trusted Platform Module -- Part 1: Overview
- ISO/IEC 11889-2:2009 Information technology -- Trusted Platform Module -- Part 2: Design principles
- ISO/IEC 11889-3:2009 Information technology -- Trusted Platform Module -- Part 3: Structures
- ISO/IEC 11889-4:2009 Information technology -- Trusted Platform Module -- Part 4: Commands
- ISO/IEC 13888-1:2009 Information technology -- Security techniques -- Non-repudiation -- Part 1: General
- ISO/IEC 13888-2:2010 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques
- ISO/IEC 13888-3:2009 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques
- ISO/IEC TR 14516:2002
- Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services
- ISO/IEC 14888-1:2008 Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General
- ISO/IEC 14888-2:2008 Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Integer factorization based mechanisms
- ISO/IEC 14888-3:2006 Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms
- ISO/IEC 14888-3:2006/Amd 1:2010 Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm Optimizing hash inputs
- ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
- ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
- ISO/IEC TR 15443-1:2012 Information technology -- Security techniques -- Security assurance framework -- Part 1: Introduction and concepts
- ISO/IEC TR 15443-2:2012 Information technology -- Security techniques -- Security assurance framework -- Part 2: Analysis
- ISO/IEC TR 15446:2009 Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets
- ISO/IEC 15816:2002 Information technology -- Security techniques -- Security information objects for access control
- ISO/IEC 15945:2002 Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures
- ISO/IEC 15946-1:2008 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General
- ISO/IEC 15946-5:2009 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation
- ISO/IEC WD 17825 Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

- ISO/IEC WD 17922 Telebiometric authentication framework using biometric hardware security module (ITU-T X.bhsm | ISO/IEC xxxxx)
- ISO/IEC 18014-1:2008 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework
- ISO/IEC 18014-2:2009 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens
- ISO/IEC 18014-3:2009 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens
- ISO/IEC CD 18014-4 Information technology -- Security techniques -- Time-stamping services -- Part 4: Traceability of time sources
- ISO/IEC 18028-3:2005 Information technology -- Security techniques -- IT network security -- Part 3: Securing communications between networks using security gateways
- ISO/IEC 18028-4:2005 Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access
- ISO/IEC 18028-5:2006 Information technology -- Security techniques -- IT network security -- Part 5: Securing communications across networks using virtual private networks
- ISO/IEC 18031:2011 Information technology -- Security techniques -- Random bit generation
- ISO/IEC 18032:2005 Information technology -- Security techniques -- Prime number generation
- ISO/IEC 18033-1:2005 Information technology -- Security techniques -- Encryption algorithms -- Part 1: General
- ISO/IEC WD 18033-1 Information technology -- Security techniques -- Encryption algorithms -- Part 1: General
- ISO/IEC 18033-2:2006 Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers
- ISO/IEC 18033-3:2010 Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
- ISO/IEC 18033-4:2011 Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers
- ISO/IEC WD 18033-5 Information technology -- Security techniques -- Encryption algorithms -- Part 5: Identity-based ciphers
- ISO/IEC 18043:2006 Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems
- ISO/IEC 18045:2008 Information technology -- Security techniques -- Methodology for IT security evaluation
- ISO/IEC WD 18367 Cryptographic algorithms and security mechanisms conformance testing
- ISO/IEC WD 18370-1 Information technology -- Security techniques -- Blind digital signatures -- Part 1: General
- ISO/IEC WD 18370-2 Information technology -- Security techniques -- Blind digital signatures -- Part 2: Discrete logarithm based mechanisms
- ISO/IEC 19772:2009 Information technology -- Security techniques -- Authenticated encryption
- ISO/IEC 19790:2012 Information technology -- Security techniques -- Security requirements for cryptographic modules
- ISO/IEC TR 19791:2010 Information technology -- Security techniques -- Security assessment of operational systems
- ISO/IEC 19792:2009 Information technology -- Security techniques -- Security evaluation of biometrics
- ISO/IEC TR 20004:2012 Information technology -- Security techniques -- Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
- ISO/IEC DIS 20008-1 Information technology -- Security techniques -- Anonymous digital signatures -- Part 1: General

- ISO/IEC DIS 20008-2 Information technology -- Security techniques -- Anonymous digital signature -- Part 2: Mechanisms using a group public key
- ISO/IEC DIS 20009-1 Information technology -- Security techniques -- Anonymous entity authentication -- Part 1: General
- ISO/IEC DIS 20009-2 Information technology -- Security techniques -- Anonymous entity authentication -- Part 2: Mechanisms based on signatures using a group public key
- ISO/IEC NP 20009-3 Information technology -- Security techniques -- Anonymous entity authentication -- Part 3: Mechanisms based on blind signatures
- ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)
- ISO/IEC 24745:2011 Information technology -- Security techniques -- Biometric information protection
- ISO/IEC DIS 24759 Information technology -- Security techniques -- Test requirements for cryptographic modules
- ISO/IEC 24759:2008 Information technology -- Security techniques -- Test requirements for cryptographic modules
- ISO/IEC 24760-1:2011 Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts
- ISO/IEC CD 24760-2 Information Technology -- Security Techniques -- A Framework for Identity Management -- Part 2: Reference architecture and requirements
- ISO/IEC WD 24760-3 Information Technology -- Security Techniques -- A Framework for Identity Management -- Part 3: Practice
- ISO/IEC 24761:2009 Information technology -- Security techniques -- Authentication context for biometrics
- ISO/IEC WD 24762 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services
- ISO/IEC 24762:2008 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services
- ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- ISO/IEC DIS 27001 Information technology -- Security techniques -- Information security management systems -- Requirements
- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements
- ISO/IEC DIS 27002 Information technology -- Security techniques -- Code of practice for information security controls
- ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management
- ISO/IEC 27003:2010 Information technology -- Security techniques -- Information security management system implementation guidance
- ISO/IEC 27004:2009 Information technology -- Security techniques -- Information security management -- Measurement
- ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management
- ISO/IEC WD 27006 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27006:2011 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

- ISO/IEC 27007:2011 Information technology -- Security techniques -- Guidelines for information security management systems auditing
- ISO/IEC TR 27008:2011 Information technology -- Security techniques -- Guidelines for auditors on information security controls
- ISO/IEC NP 27009 The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications
- ISO/IEC 27010:2012 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011:2008 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013:2012 Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC FDIS 27014 Information technology -- Security techniques -- Governance of information security
- ISO/IEC TR 27015:2012 Information technology -- Security techniques -- Information security management guidelines for financial services
- ISO/IEC PDTR 27016 Information technology -- Security techniques -- Information security management -- Organizational economics
- ISO/IEC WD 27017 Information technology -- Security techniques -- Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002
- ISO/IEC WD 27018 Code of practice for data protection controls for public cloud computing services
- ISO/IEC DTR 27019 Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry
- ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity
- ISO/IEC 27033-1:2009 Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts
- ISO/IEC WD 27033-1 Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts
- ISO/IEC 27033-2:2012 Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security
- ISO/IEC 27033-3:2010 Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues
- ISO/IEC DIS 27033-4 Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways
- ISO/IEC DIS 27033-5 Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Network (VPNs)
- ISO/IEC WD 27033-6 Information technology -- Security techniques -- Network security -- Part 6: Securing IP network access using wireless
- ISO/IEC 27034-1:2011 Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts
- ISO/IEC WD 27034-2 Application security -- Part 2: Organization normative framework
- ISO/IEC NP 27034-3 Application security -- Part 3: Application security management process
- ISO/IEC NP 27034-4 Application security -- Part 4: Application security validation
- ISO/IEC WD 27034-5 Application security -- Part 5: Protocols and application security controls data structure

- ISO/IEC WD 27034-6 Application security -- Part 6: Security guidance for specific applications
- ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management
- ISO/IEC WD 27035-1 Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management
- ISO/IEC WD 27035-2 Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines for incident response readiness
- ISO/IEC WD 27035-3 Information technology -- Security techniques -- Information security incident management -- Part 3: Guidelines for CSIRT operations
- ISO/IEC DIS 27036-1 Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts
- ISO/IEC DIS 27036-2 Information technology -- Security techniques -- Information security for supplier relationships -- Part 2: Common requirements
- ISO/IEC DIS 27036-3 Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for ICT supply chain security
- ISO/IEC WD 27036-4 Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of outsourcing
- ISO/IEC 27037:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC DIS 27038 Information technology -- Security techniques -- Specification for Digital Redaction
- ISO/IEC CD 27039 Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems
- ISO/IEC CD 27040 Information technology -- Security techniques -- Storage security
- ISO/IEC CD 27041 Guidance on assuring suitability and adequacy of investigation methods
- ISO/IEC CD 27042 Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC CD 27043 Investigation principles and processes
- ISO/IEC WD 27044 Security Information and Event Management (SIEM)
- ISO/IEC WD 29003 Identity proofing
- ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework
- ISO/IEC DIS 29101 Information technology -- Security techniques -- Privacy architecture framework
- ISO/IEC 29115 Information technology -- Security techniques -- Entity authentication assurance framework
- ISO/IEC 29128:2011 Information technology -- Security techniques -- Verification of cryptographic protocols
- ISO/IEC WD 29134 Privacy impact assessment
- ISO/IEC WD 29146 Information technology - Security techniques - A framework for access management
- ISO/IEC DIS 29147 Information technology - Security techniques - Vulnerability disclosure
- ISO/IEC TR 29149:2012 Information technology -- Security techniques -- Best practices for the provision and use of time-stamping services
- ISO/IEC 29150:2011 Information technology -- Security techniques -- Signcryption
- ISO/IEC WD 29190 Proposal on Privacy capability assessment model
- ISO/IEC 29191:2012 Information technology -- Security techniques -- Requirements for partially anonymous, partially unlinkable authentication.
- ISO/IEC 29192-1:2012 Information technology -- Security techniques -- Lightweight cryptography -- Part 1: General
- ISO/IEC 29192-2:2012 Information technology -- Security techniques -- Lightweight cryptography -- Part 2: Block ciphers

- ISO/IEC 29192-3:2012 Information technology -- Security techniques -- Lightweight cryptography -- Part 3: Stream ciphers
- ISO/IEC FDIS 29192-4 Information technology -- Security techniques -- Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques
- ISO/IEC PDTR 29193 Secure system engineering principles and techniques
- ISO/IEC PDTS 30104 Information Technology -- Security Techniques -- Physical Security Attacks, Mitigation Techniques and Security Requirements
- ISO/IEC DIS 30111Information technology - Security techniques - Vulnerability handling processes
- ISO/IEC WD TR 30127 Information technology -- Security techniques -- Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis

Annex C Liaisons to ISO SC 27

Please note that liaison change constantly therefore this list may not be current.

ISO committees in liaison:

- TC 8 Ships and maritime technology
- TC 46/SC 11 Archives/records management
- TC 68/SC 2 Financial services, security
- TC 68/SC 7 Core Banking
- TC 176/SC 3 Supporting technologies
- TC 204 Intelligent transport systems
- TC 215 Health informatics
- TC 223 Societal security
- TC 247 Fraud countermeasures and controls
- TC 251 Project committee: Asset management
- TC 259 Project committee: Outsourcing
- CASCO Committee on conformity assessment

IEC committees in liaison:

- IEC/TC 57 Power systems management and associated information exchange
- IEC/TC 65 Industrial-process measurement, control and automation

Organizations in liaison:

- Common Criteria Development Board (CCDB)
- Common Study Center of Telediffusion and Telecommunication (CCETT)
- Cloud security alliance
- European Committee for Banking Standards (ECBS)
- European Network and Information Security Agency (ENISA)
- European Payments Council (EPC)
- European Telecommunications Standards Institute (ETSI)
- Ecma International – European association for standardizing information and communications systems
- Information Systems Audit and Control Association/ IT Governance Institute (ISACA/ITGI)
- International Systems Security Engineering Association (ISSEA)
- International Telecommunication Union (ITU)
- MasterCard
- Visa