The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number: **NIST Interagency Report (NISTIR) 8074 Volume 2**

Title: **Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity**

Publication Date: **December 2015**

- Final Publication: http://dx.doi.org/10.6028/NIST.IR.8074v2 (which links to http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf)
- Related Information on CSRC: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8074v2
- Information on other NIST cybersecurity publications and programs can be found at: http://csrc.nist.gov/

The following information was posted with the attached DRAFT document:

Aug. 10, 2015

NIST IR 8074

DRAFT Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (2 Volumes):
Volume 1: Report
Volume 2: Supplemental Information for the Report

NIST seeks public comments on Draft NIST Interagency Report (NISTIR) 8074, which comprises two volumes, “Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity” (Vol. 1) and “Supplemental Information” (Vol. 2).

The public comment period closed September 24, 2015.

NISTIR 8074 Volume 2 (Draft)

Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

Editors:
Michael Hogan
Elaine Newton

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.xxxx

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8074 Volume 2 (Draft)

Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

Editors:
Michael Hogan
Elaine Newton
Office of the Director
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.xxxx

August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency Report 8074 Volume 2
(Draft)
87 pages (August 2015)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.xxxx

Certain commercial entities may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities are necessarily the best available for the purpose.

Public comment period: *August 10, 2015* through *September 24, 2015*

National Institute of Standards and Technology
Attn: Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir8074@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

This report provides background information and analysis in support of NISTIR 8074 Volume 1, *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*. It provides a current summary of ongoing activities in critical international cybersecurity standardization and an inventory of U.S. Government and U.S. private sector engagement. It also provides information for federal agencies and other stakeholders to help plan more effective participation in international cybersecurity standards development and related conformity assessment activities.

Keywords

conformity assessment; coordination; cybersecurity; ICS; Industrial Control Systems; international standards; IT; information technology; privacy; standards education; strategy; SDO; standards developing organizations; standards development

Foreword

This Supplemental Information document has been developed by the International Cybersecurity Standardization Working group established by the National Security Council-led Cybersecurity Interagency Policy Committee. It provides background information and analysis in support of the *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*. It provides a current summary of ongoing activities in critical international cybersecurity standardization and an inventory of USG and U.S. private sector engagement. It also provides information for federal agencies and other stakeholders to help plan more effective participation in international cybersecurity standards development and related conformity assessment activities.

Table of Contents

Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

Introduction

Use of cybersecurity standards for information technologies (IT)[1] and industrial control systems (ICS) are necessary for the cybersecurity and resiliency of all U.S. information and communications systems and supporting infrastructures. This document provides additional information that supports the strategic objectives and recommendations in the report: *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*.

Additionally, widespread awareness of the topics covered in this document will inform U.S. policymakers, enhance the effectiveness of standards engagement by agency cybersecurity standards participants and their management, and support cooperative activities between and among agencies, with other governments and the private sector. Such topics include: the nature of international standards development and types of conformity assessment; the role of international cybersecurity standards and conformity assessment in enhancing security and promoting commerce; an inventory of critical cybersecurity standards developing organizations (SDOs) and the status of cybersecurity standards in core areas; ongoing issues in IT standardization; and general principles for effective participation in standards development, including in situations where accelerating standards development is desirable.

This document does not attempt to establish authoritative definitions for key terms, some of which have been defined more than once by other bodies. For purposes of this document, working definitions for key terms are found in Annex A.

Conformity Assessment, which evaluates whether a product, process, or service fulfills a given set of requirements, is discussed within the body of this document and explained in more depth in Annex B.

In support of the document's analysis of the status of cybersecurity standardization for critically important IT applications, Annex C lists USG mandates relating to cybersecurity, and Annex D provides cybersecurity analyses for some key and emerging IT application areas.

Annex E provides a summary of ongoing activities in critical cybersecurity SDOs and the present level of USG and U.S. private sector engagement.

This document does not address USG use of these standards in regulation, procurement, or other mission-related activities. That topic is covered by OMB Circular A-119.

[1] Also referred to as Information and Communications Technologies (ICT).

1 Why are cybersecurity standards critical?

"America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas." [2]

With the convergence and connectivity of IT, the deployment of cybersecurity standards-based products, processes, and services is essential. Establishment and use of international cybersecurity standards are essential for: improving trust in online transactions, mitigating the effects of cyber incidents (e.g., crime), and ensuring secure interoperability among trade partners, thereby facilitating increased efficiencies in the global economy. Such standards are especially important in the interconnected world where products, processes, and services are developed and delivered throughout global supply chains that provide acquirers little transparency into supplier practices beyond the prime contractor. A recent report on the economic costs of cybercrime[3] stated:

> "Cybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest of these figures is more than the national income of most countries and governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow."

International standardization can also be used as a competitive tool. Firms often have well-defined strategies for standards development, including management of intellectual property rights, aimed at achieving that advantage. Advantage can be gained by influencing the development of a standard. In some cases, firms can gain a competitive advantage by being first to market with a standards-based product, process, or service.

Finally, Federal agencies rely heavily on voluntary consensus standards – including international standards -- which they often incorporate into regulatory and procurement requirements or use in support of other mission-related activities. Occasionally, standards-related measures are used by countries to protect domestic producers or provide a competitive advantage, or such measures can distort trade for other reasons as well. The World Trade Organization (WTO) Agreement, including the WTO Agreement on Technical Barriers to Trade (TBT Agreement), and other trade agreements establish rules governing the use of standards-related measures by governments to ensure that such measures are not used in a manner that discriminates against foreign products or otherwise creates unnecessary obstacles to trade.

---

[2] President Obama, see https://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

[3] McAfee, Inc.: Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies, June 2014.

2 Why is conformity assessment for cybersecurity standards important?

"When you can measure what you are speaking about and express it in numbers, you know something about it; but when you cannot measure, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science." [4]

When protecting sensitive information and networks, government agencies need to have a minimum level of assurance that a stated security claim is valid. Conformity assessment (CA) determines whether a product, process, or service has fulfilled the specified requirements, including those contained in a standard. There are several types and numerous possible combinations of CA – see Annex B for an overview – but, in the field of IT, testing is often the most rigorous way to determine if a product, process, or service has fulfilled all of the requirements. An example is the USG requirement of using tested and validated cryptographic modules.[5]

A user's (e.g., a regulator) confidence in test results may be influenced by the level of independence of the testing body (e.g., first, second, or third party) and/or recognition by an accrediting body. This in turn directly relates to the risk associated with product, process, or service non-conformance. For IT, the three most important types of conformity assessment-related testing are: conformance, performance, and interoperability testing.

- *Conformance testing* captures the technical description of the requirements in a standard and measures whether an implementation (product, process, or service) faithfully fulfills these requirements. Conformance testing does not completely ensure the interoperability or performance of conforming products, processes, or services. Therefore, interoperability and performance testing are also important aspects for procurements.

- *Performance testing* measures the performance characteristics of an implementation, such as its throughput or responsiveness, under various conditions.

- *Interoperability testing* tests one implementation with another to establish that they can work together properly.

Testing, and ensuring the competence of bodies that conduct the testing, is as much of a market driver as the specific standard itself. In support of international trade, the TBT Agreement encourages mutual acceptance of test results of conformity assessment procedures and the use of international systems of conformity assessment.

Other types of CA are often used to ensure that products, processes, or services comply with regulations or voluntary consensus standards. These include: tests of components, certification of test results, and accreditation methods that assess the competence of testing, certification, and inspection bodies. Using commercial testing bodies known to be competent for specific testing areas can be more cost effective for Federal agencies than developing USG testing expertise.

[4] Lord Kelvin, William Thomson, a British scientist who helped to lay the foundations of modern physics. Lecture on "Electrical Units of Measurement" (3 May 1883), published in *Popular Lectures* Vol. I, p. 73

[5] NIST Cryptographic Module Validation Program (CMVP)

3 Core Areas in Cybersecurity Standardization

Core areas are key attributes of cybersecurity that broadly impact the overall cybersecurity of IT products, processes, and services. Core areas of cybersecurity standardization include:

Cryptographic Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.

Cyber Incident Management standards support information sharing processes, products, and technology implementations for cyber incident identification, handling, and remediation. Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident and recover from any losses as a result of the incident. It allows jurisdictions to exchange information about incidents, vulnerabilities, threats and attacks, the system(s) that were exploited, security configurations and weaknesses that could be exploited, etc.

Identity Management and related standards enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.

Information Security Management System (ISMS) standards provide a set of processes and corresponding security controls to establish a governance structure for information security for an organization, an organizational unit, or a set of processes controlled by a single organizational entity. An ISMS requires a risk-based approach to security that involves selecting specific security controls based on the desired risk posture of the organization and requires measuring effectiveness of security processes and controls. An ISMS requires a cycle of continual improvement for an organization to continue assessing security risks, assessing controls, and improving security to remain within risk tolerance levels.

IT System Security Evaluation and assurance standards are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.

Network Security standards provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and internet.

Security Automation and Continuous Monitoring (SACM) standards describe protocols and data formats that enable the ongoing, automated collection, monitoring, verification, and maintenance of software, system, and network security configurations, and provide greater awareness of vulnerabilities and threats to support organizational risk management decisions. Automation protocols also include standards for machine-readable vulnerability identification and metrics, platform and asset identification, actionable threat information and policy triggers for actions to respond to threats and policy violations

Supply Chain Risk Management (SCRM) standards provide the confidence that organizations will produce and deliver information technology products or services that perform as required and mitigate supply chain-related risks, such as the insertion of counterfeits and malicious software, unauthorized production, tampering, theft, and poor quality products and services. IT SCRM standardization requirements include methodologies and processes that enable an organization's increased visibility into, and understanding of, how technology that they acquire and manage is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. IT SCRM standardization lies at the intersection of cybersecurity and supply chain management and provides a mix of mitigation strategies from both disciplines for a targeted approach to managing IT supply chain risks.

Software Assurance standards describe requirements and guidance for ensuring software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This includes custom software, commercial off-the-shelf software, firmware, operating systems, utilities, databases, applications and applets for the Web, software/platform/infrastructure as a service (SaaS, PaaS, IaaS), mobile and consumer devices, etc.

System Security Engineering standards describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.

4 Some Key IT Applications

IT applications are systems that support performing real-world tasks, which benefit organizations and people. Present USG priorities in IT applications are driven by agencies' missions and specific legislative and policy mandates, which are listed in Annex C. Based upon the mandates listed in Annex C, some of the high priority IT applications for the USG are described below. A cybersecurity analysis of each of these IT application areas is contained in Annex D.

Cloud Computing Cloud computing is a relatively new paradigm that changes the emphasis of the traditional IT services from procuring, maintaining, and operating the necessary hardware and related infrastructure to the business' mission, and delivering value added capabilities and services at lower cost to users. Defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction, cloud computing maximizes capacity utilization, improves IT flexibility and responsiveness, and minimizes cost of implementations and operations for all cloud-based information systems.

Emergency Management The first responder community needs reliable, secure, and interoperable information and communications technology to protect the public during disasters and catastrophes. There is increasing convergence of the voice, data, and video information being exchanged to provide situational awareness in response to an event. For larger disasters and catastrophes, first responders from neighboring jurisdictions or inter-governmental jurisdictions (i.e., state or Federal) need to be integrated into the response, along with the information and communications technologies they use.

Industrial Control Systems (ICS) ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations often found in the industrial control sectors. ICSs are used across the critical infrastructure and key resources (CIKR) sectors, including the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and critical manufacturing (automotive, aerospace, and durable goods) industries.

Health Information Technology (HIT) The use of information technology makes it possible for health care providers to better manage patient care through secure use and sharing of health information. HIT includes the use of electronic health records (EHRs) instead of paper medical records to maintain patient health information and to support and manage their clinical care. Secure and interoperable HIT provides for: seamless movement between health care providers without loss of information; instant access to medical histories at the point of care; fewer errors and redundant tests; more efficient and effective reporting, surveillance, and quality monitoring; and quick detection of adverse drug reactions and epidemics.

Smart Grid The electric power industry is undergoing grid modernization efforts to transform from a centralized, producer-controlled network to one that is a distributed and consumer-interactive grid that enables bidirectional flows of energy and uses two-way communication and control capabilities. The move to a smarter electric grid will provide new ways in which power can be generated, delivered and used that minimize environmental impacts, improve reliability and service, reduce costs and improve efficiency. Deployment of various Smart Grid elements, including smart sensors on distribution lines, smart meters in homes, and integration of widely dispersed sources of renewable energy, is already underway and further integrates the energy, IT and telecommunication sectors.

Voting The most familiar part of a voting system is the mechanism used to capture the citizenry's choices or votes on ballots. In addition to the vote capture mechanism, a voting system includes voter registration databases and election management systems. Voter registration databases contain the list of citizens eligible to participate in a jurisdiction's election. Voter registration databases populate poll books used at polling places to verify one's eligibility to participate in an election and ensure they received the correct ballot style. The election management system is used to manage the definition of different ballot styles, configuration of the vote capture mechanism, collection and tallying of cast ballots, and creation of election reports and results.

5 Present State of International Cybersecurity Standardization

The status of cybersecurity standards can be assessed by reviewing some key USG priority IT applications, which are described in Section 4 and Annex D with respect to the core areas of cybersecurity standardization that are described in Section 3.

Table 1 below provides a snapshot of the present status of cybersecurity standards and their implementation by the marketplace. "Standards Mostly Available" indicates that SDO approved cybersecurity standards are for the most part available and that standards-based implementations are available. However, the availability of standards means that such standards require continuous maintenance and updating based upon feedback from testing and deployments of standards-based products, processes, and services, as well as improvements in technology and the exploitation of those improvements by our adversaries. "Standards Being Developed" indicates that needed SDO approved cybersecurity standards are still under development and that needed standards-based implementations are not yet available. "New Standards Needed" indicates that many needed cybersecurity standards are at the beginning stages of development within various SDOs and therefore standards-based implementations are not yet available. Where there are existing standards that are being implemented, it should be noted that these standards will also need to be maintained and replaced, particularly as new technologies evolve.

Cybersecurity standards include many standards that are much broader than cybersecurity but are very relevant to cybersecurity, as well as standards whose scopes are specific to one or more attributes of cybersecurity. It is important to highlight that there are a number of generic standards under development or in existence that are relevant to the core area rows and specific applications in the columns of Table 1 below. Given that context, based upon the information in Table 1, a couple of observations can be made on the overall status of ongoing cybersecurity standardization. First, the listed core areas of cybersecurity standardization have been, are, and undoubtedly will be necessary for the deployment of IT that is interoperable, secure and resilient. Second, as illustrated by the listed IT applications, there is a mix of ongoing standardization and maintenance of recently approved standards that is necessary to sustain deployments of standards-based IT products, processes and services. Consequently, the USG needs to maintain its core competency in these core areas, which requires a critical mass of experts from the agencies. To do this over the long term, the USG should include in its strategic planning a focus on its cybersecurity standardization activity.

Core Areas of Cybersecurity Standardization	Examples of Relevant Standards Developers	Examples of Some Key IT Applications					
		Cloud Computing	Emergency Management	Industrial Control Systems	Health IT	Smart Grid	Voting
Cryptographic Techniques	IEEE ISO TC 68 ISO/IEC JTC 1 W3C	Standards Mostly Available	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Being Developed
Cyber Incident Management	ISO/IEC JTC 1 ITU-T PCI	Standards Being Developed	New Standards Needed	Standards Being Developed	Standards Being Developed	Standards Being Developed	New Standards Needed
Identity Management	FIDO Alliance IETF; OASIS OIDF ISO/IEC JTC 1 ITU-T; W3C	Standards Mostly Available	Standards Being Developed	New Standards Needed	Standards Being Developed	New Standards Needed	New Standards Needed
Information Security Management Systems	ATIS IEC ISA ISO/IEC JTC 1 OASIS ISO TC 223	Standards Being Developed	New Standards Needed	Standards Being Developed	Standards Being Developed	New Standards Needed	New Standards Needed
IT System Security Evaluation	ISO/IEC JTC 1	Standards Being Developed	Standards Mostly Available	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Mostly Available
Network Security	3GPP; 3GPP; IEC IETF; IEEE ISO/IEC JTC 1 ITU-T WiMAX Forum	New Standards Needed	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Mostly Available
Security Automation & Continuous Monitoring	IETF ISO/IEC JTC 1 TCG	Standards Being Developed	Standards Being Developed	New Standards Needed	Standards Being Developed	New Standards Needed	New Standards Needed
Software Assurance	IEEE ISO/IEC JTC 1 TCG	New Standards Needed	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Being Developed	Standards Being Developed
Supply Chain Risk Management	ISO/IEC JTC 1 The Open Group IEC TC 65	Standards Being Developed	New Standards Needed	Standards Being Developed	New Standards Needed	New Standards Needed	New Standards Needed
System Security Engineering	IEC ISA ISO/IEC JTC 1	New Standards Needed	Standards Mostly Available	Standards Being Developed	Standards Being Developed	New Standards Needed	Standards Being Developed

Table 1 Status of Cybersecurity Standardization in Core Areas (Illustrative Examples)

Table 2 below provides a proposed classification system that the interagency can utilize for characterizing the maturity level of particular standards, which will help inform any discussions of prioritization and strategy.

Note that some SDOs require two or more implementations before final approval of a standard. Such implementations may or may not be commercial products or services. In other cases, an SDO may be developing a standard while conforming commercial products or services are already being sold. Innovation in IT means that IT standards are constantly being developed, approved, and maintained. Revisions to previous editions of standards may or may not be backward-compatible. An SDO approved standard does not necessarily equate with success. Widespread market acceptance of an approved standard is the ultimate goal.

Maturity Level	Definition
No Standard	SDOs have not initiated any standard development projects.
Under Development	SDOs have initiated standard development projects. Open source projects have been initiated.
Approved Standard	SDO-approved standard is available to public. Some SDOs require multiple implementations before final designation as a “standard.”
Technically Stable	The standard is stable and its technical content is mature. No major revisions or amendments are in progress that will affect backward compatibility with the original standard.
Reference Implementation	Reference implementation is available.
Testing	Test tools are available. Testing and test reports are available.
Commercial Availability	Several products/services from different vendors exist on the market to implement this standard.
Market Acceptance	Widespread use by many groups. De facto or de jure market acceptance of standards-based products/services.
Sunset	Newer standards (revisions or replacements) are under development.

Table 2 An IT Standards Maturity Model

5.1 A High-Level Standards Status Analysis of the IT Applications in Table 1

Cloud Computing The adoption of a cloud-based solution does not inherently provide for the same level of security, privacy and compliance with mandates that were achieved in the traditional IT model of the information system. From the risk assessment process, through the identification of the risk mitigation mechanisms, to the continuous monitoring (diagnosis and mitigation), cloud computing ecosystems bring to consumers new challenges that need to be addressed before cloud consumers can full take advantage of this new technology benefit. The transition from distributed systems for which system owners have full control and management capabilities available, to the utility-like resources provided by cloud computing ecosystems, requires cybersecurity standards that address technical, policy and regulatory issues for security, privacy and forensics in the cloud.

In a cloud ecosystem, a cloud consumer's ability to comply with any business, regulatory, operational, or security requirements in a cloud computing environment is a direct result of the service and deployment model adopted by the agency, the cloud architecture, and the deployment and management of the resources in the cloud environment. Leveraging NIST's initial cloud computing definition and architecture, the two international standards developers have developed and approved a standardized cloud vocabulary [ISO/IEC 17788 | Recommendation ITU-T Y.3500], and a cloud architecture [ISO/IEC 17789 | Recommendation ITU-T Y.3502]. These standards create a strong foundation for the majority of the current cloud standards development, such as Cloud Security Assessment and Audit, Application Security Validation [ISO/IEC 27034-4], electronic Discovery [ISO/IEC 27050], Service Level Agreement Framework – Part 4: Security and Privacy [ISO/IEC 19086-4], to list a few of them. Other architectural efforts come from the OpenStack Foundation. OpenStack is an open source set of software tools for building and managing cloud computing platforms for public and private clouds.

However, in order to authorize the use of a cloud-based information system, cloud consumers are required to build trust into the acquired cloud service, and into the cloud provider as a business partner. A well-defined, repeatable, risk assessment process provides the foundation for trust establishment and can only be achieved when a corresponding level of transparency into the cloud service offering is achieved. While existing standards that address the information security management systems exist for information systems that are directly managed and controlled by system-owners and are also applicable to cloud providers or cloud brokers, equivalent standards that provide guidance to consumers that need to gauge the risk incurred when adopting cloud-based solutions remain to be developed by SDOs.

The communication between end-users and cloud ecosystem is supported by existing standards that have been developed to facilitate communication, data exchange, and security, such as base-level infrastructure standards, (e.g., TCP/IP, DNS, SMTP, HTML, HTTP, HTTPS, FTP,) These standards offer a convenient and secure access to cloud-based information systems, while restricting majority security exposures of data in transit. Other standards such as SSL and TLS provide public-key cryptographic protocols that allow customers and cloud providers to automatically establish shared keys that can be used to protect their communications (although much yet remains to be done in this space).

Other security standards that are relevant to cloud computing include XACML (eXtensible Access Control Markup Language) and SAML (Security Assertion Markup Language). A number of additional web-oriented standards exist, including the WS (Web Services) standards such as WS-Trust, WS-Policy, WS-SecurityPolicy, etc., but their adoption by the market place is limited.

Existing standards such as XML (eXtensible Markup Language) - a central standard for describing structured data and sharing it between possibly dissimilar systems – can support data portability in the cloud, while existing higher-level standards such as WSDL (Web Services Definition Language) and SOAP (Simple Object Access Protocol) that help web users locate and access web-based services are employed by many cloud providers in a building-blocks approach.

The Open Virtualization Format (OVF) from the Distributed Management Task Force (DMTF) is an open standard for packaging and distributing virtual appliances or more generally software to be run in virtual machines. The standard describes an "open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines". Because the OVF v1.1 standard is not tied to any particular hypervisor or processor architecture, ISO/IEC JTC1 adopted it as international standard in August 2011.

In sum, cloud computing can greatly benefit from carefully considered new standards. While current standards are being proven able to foster the rapid development of a cloud market place of competing but mostly incompatible products and services, standards are needed to supply privacy, security, portability, interoperability, forensics support, service level agreements (SLA) and metrics for cloud-based information systems. Key areas needing new cloud-oriented standards are: risk management, conformity assessment, security service level agreements, security metrics, continuous monitoring, privacy, and forensics (including electronic discovery).

Emergency Management First responders use private, land mobile radio systems for their mission critical voice communications. These networks are designed and built on a set of standards and user requirements that address critical operational concerns, including user authentication, security and reliability. With emergence of broadband applications and services, first responders are beginning to incorporate broadband data applications into their day-to-day operations. As a result of this uptake of IP-based services, first response agencies must incorporate cybersecurity planning into their minimum level functional requirements.

First responders are in the initial stages of planning for and adopting a nationwide wireless broadband network in the 700 MHz spectrum band to provide voice and data capabilities. The technology standard of choice, Long Term Evolution (LTE), which is based on an all-IP architecture, will introduce both new capabilities and new, significant risks to public safety. Consequently, cybersecurity policies that are national in scope must be adopted across the community to ensure adequate security and mitigate cyber-attacks.

Unfortunately, developing national cybersecurity policies for first responders will prove difficult, as there are more than 50,000 state and local public safety entities across the United States with varying interests and missions. Aside from the difficulty associated with achieving consensus on what these policies should be, it would be equally challenging to ensure uniform implementation across the Nation. However, there are many areas within the emergency response community that require cybersecurity standards, such as records management systems, geo-spatial information, and secure communications over wired and wireless networks. (The First Responder Network Authority (FirstNet) was created on Feb 22, 2012. It will use 700MHz spectrum and the Long-Term Evolution (LTE) standards in order to provide a nationwide interoperable first responder communications system.)

At the Federal level, agencies such as the Department of Homeland Security and the Department of Justice have policy directives in place that mandate specific cybersecurity requirements; however, state and local first responder agencies do not have the same cybersecurity requirements, if any at all. Additionally, because emergency communications operate over private networks, there is less incentive for state and local agencies to adopt or implement cybersecurity techniques as doing so would increase cost on severely constrained budgets.

Industrial Control Systems (ICS) In order to securely design, develop, implement, and maintain cybersecurity in industrial control systems (ICS), the development and application of existing and new standards is needed. The Industrial Society of Automation (ISA), through the ISA99 committee, is developing and establishing standards, technical reports and related information that will define procedures for implementing electronically secure industrial automation and control systems, security practices, and assessing electronic security performance. This suite of standards, ISA/IEC 62443: Security for Industrial Automation and Control Systems is the result of a strong collaborative relationship between ISA99 and IEC TC65 WG10. Gaps in current ICS cybersecurity standards development include finalized metrics standards and business case development to incentivize application of ICS cybersecurity standards with limited resources of ICS owners and users.

Health Information Technology Standards are necessary to implement a secure and interoperable HIT infrastructure. Many existing national and international cybersecurity standards, specifications, and technical frameworks can be applied to the HIT application area to provide core cybersecurity capabilities. However, with the increasing focus on HIT, there is a need for more mature standards that are directly applicable to, and developed within the context of this application area.

Smart Grid To address NIST's responsibility under the Energy Independence and Security Act of 2007 to coordinate development of a Smart Grid interoperability framework that includes protocols and model standards, NIST identified standards that could be immediately applied to meet Smart Grid needs or were expected to be available in the near future, and identified and established priorities and action plans to develop additional needed standards to fill these gaps. Release 3.0 of the NIST Framework and Roadmap for Smart Grid Interoperability Standards identifies 71 Smart Grid-relevant standards, 17 of which specifically address cybersecurity. However, to ensure the secure design, development, implementation, and maintenance of the Smart Grid infrastructure, there is a need to develop and apply interoperable security standards.

Voting In the United States, standards for voting systems are promulgated by the Election Assistance Commission (EAC) as the Voluntary Voting System Guidelines (VVSG), a standard developed with technical support from NIST. The EAC administers an accreditation program for testing laboratories that test the conformance of voting system equipment to the requirements found in the VVSG. The Institute of Electrical and Electronics Engineers (IEEE) Voting System Standards Committee 1622 (VSSC/1622) is creating standards and guidelines around a common data format (CDF) for election data so that election equipment used in U.S. elections and interfacing software can interoperate more easily. The Organization for the Advancement of Structured Information Standards (OASIS) has established a technical committee on Election and Voter Services that has produced the Election Markup Language (EML) based on the Extensible Markup Language (XML) with the goal of allowing hardware, software, and service providers of election system and service providers to exchange information.

5.2 A High-Level Standards Status Analysis of the Cybersecurity Core Areas in Table 1

Cryptographic Techniques Cryptographic algorithm standards have been widely available for some time. For example, the Advanced Encryption Standard (AES) block cipher is included in ISO/IEC 18033-3:2010, is the preferred block cipher for IEEE 802.11 to secure wireless networks, and is required to implement in version 1.2 of the IETF's Transport Layer Security (TLS) protocol.

Public key cryptography standards have also been widely available. The Internet Engineering Task Force has been developing public key cryptography standards for Internet applications. The IEEE 1363 working group has been publishing standards for public key cryptography, including IEEE 1363-2000, IEEE 1363a, IEEE P1363.1, and IEEE P1363.2.

Lightweight cryptography standards are needed for emerging areas in which highly constrained devices are interconnected, typically communicating wirelessly with one another, working in concert to accomplish some task. Examples of these areas include: sensor networks, healthcare, distributed control systems, the Internet of Things (IoT), cyber-physical systems, and the smart grid. Security and privacy can be very important in all of these areas. Because the majority of modern cryptographic algorithms were designed for desktop/server environments, many of these algorithms cannot be implemented in the devices used by these applications. When current algorithms can be engineered to fit into the limited resources of constrained environments, their performance is typically not acceptable.

Some relevant standards are:

- ISO/IEC 29192-1: 2012-06-15, (1st edition) Lightweight cryptography - Part 1: General
- ISO/IEC 29192-2: 2012-01-15, Lightweight cryptography - Part 2: Block ciphers (1st edition)
- ISO/IEC 29192-3: 2012-10-01 (1st edition), Lightweight cryptography - Part 3: Stream ciphers
- ISO/IEC 29192-4: 2013-06-01 (1st edition), Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques
- ISO/IEC 29192-4:2013/Amd.1: (2014), Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques
- 1st CD 29192-5, Lightweight cryptography - Part 5: Hash-functions

Where lightweight cryptography standards are needed to support constrained, interconnected devices, "Standards Being Developed" appears in Table 1 for this core area.

Cyber Incident Management While higher level standards for cyber incident management are available, emerging low-level standards and implementations are under development that will facilitate the automated exchange of incident-related data such as indicators of compromise;

tactics, techniques, and procedures (TTPs); threat actors; and courses of action. Existing standards include:

- ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management
- ITU-T X.1056 Security incident management guidelines for telecommunications organizations
- Payment Card Industry (PCI) Data Security Standard (DSS) v3

Emerging standards include:

- IETF RFC 4765 Intrusion Detection Message Exchange Format (IDMEF)
- IETF RFC 5070 Incident Object Description Exchange Format (IODEF)
- IETF RFC 5901 Extensions to the IODEF for Reporting Phishing
- IETF RFC 6545 Real-time Inter-network Defense (RID)
- Structured Threat Information Expression (STIX)
- Trusted Automated Exchange of Indicator Information (TAXII)
- Cyber Observable eXpression (CybOX)

Therefore, "Standards Being Developed" or "New Standards Needed" appears in Table 1 for this core area.

Identity Management There are significant identity management standards that comprise risk management techniques and specifications to assert identity and authentication, as well as enforce access policy on a range of platforms. Mature enterprise standards such as Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML) and the family of PKI cryptographic techniques to authenticate users and devices are widely deployed and in use in the cloud-computing key IT application. Emerging standards are being developed to abstract authentication form factors away from applications, allowing a rich set of strong credentials to be interoperable online.

Risk based approaches to determine assurance levels required to protect online transactions, and the associated technical and procedural controls have been adopted at the Federal level and similar standards ratified within international standards organizations. However, international government identity programs are developing their own standards and guidelines rather than adopting a smaller set of existing standards. In the private sector, industry has developed profiles to meet the needs of their business model and partners, and risk tolerance, but there is not agreement among organizations which identity assurance standard is the most holistic and therefore capable of being adopted cross-industry.

Standards to enforce access policies, share attributes, preserve anonymity, minimize data release, and consent are still immature, difficult to deploy, and not available by a large majority of SaaS providers and traditional enterprise product vendors, additionally hampering adoption.

HealthIT is in the midst of an aggressive effort to standardize authentication, consent, and authorization to medical records across patients, providers, insurers, and research entities. With the increase of commercial and enterprise internet-connected devices (IoT), standards for device identity, outside of traditional PKI, are just being researched, but the market has yet to determine what, if any that exist, will be leveraged.

Information Security Management Systems (ISMS) The ISO/IEC 27000 series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system. The fundamental parts of this series are broadly applicable to IT systems and applications.

Because of some distinctive attributes of cloud computing, several standards are being developed for cloud computing applications. These include:

- DIS 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- WD 27036 - Part 4: Guidelines for security of Cloud services
- ISO/IEC 27018:2014, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

There is a sector specific technical report for smart grid:

- ISO/IEC TR 27019:2013 (1st edition) Information security management guidelines based on ISO/IEC27002 for process control systems specific to the energy industry

There is one standard for business continuity that is relevant to emergency management:

- ISO/IEC 27031:2011 (1st edition), Guidelines for ICT readiness for business continuity

The ISA/IEC 62443 series of Industrial Automation and Control Systems (IACS) standards and technical reports includes security management requirements.

More specific standards have been and are being developed to augment existing portfolios, such as the 27000-series. This is why "Standards Being Developed" appears in Table 1 for this core area.

IT System Security Evaluation There is a growing portfolio of standards for testing and validation of cryptographic modules that are being widely applied. The third edition of ISO/IEC 19790:2015, Security requirements for cryptographic modules, will be published later this year. ISO/IEC 24759:2014, Test requirements for cryptographic modules, is the second edition. A new technical report is ready to publish: ISO/IEC TR 30104:2015, Physical security attacks, mitigation techniques and security requirements.

Draft standards include:

- DIS 17825, Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
- 1st WD 20085-1, Test tool requirements and test tool calibration methods for use in testing non-invasive attacks mitigation techniques in cryptographic modules – test tools and techniques

- 1st WD 20085-2, Test tool requirements and test tool calibration methods for use in testing non-invasive attacks mitigation techniques in cryptographic modules – test calibration methods and apparatus
- 1st CD 18367, Cryptographic algorithms and security mechanisms conformance testing
- 1st WD 19896-1, Competence requirements for information security testers and evaluators— Part 1 Introduction, concepts and general requirements
- 1st WD 19896-2, Competence requirements for information security testers and evaluators— Part 2 Knowledge, skills, and effectiveness requirements for ISO/IEC 19790 testers

Standards for the security assessment of operational systems have been revised several times. These include the three part standard ISO/IEC 15408, Information technology -- Security techniques -- Evaluation criteria for IT security.

All of these draft and mature standards are broadly applicable to the evaluation of security properties of IT products. Therefore, “Standards Being Developed” or “Standards Mostly Available” appears in Table 1 for this core area.

Network Security Many standards developers have developed and are developing network security standards. The IETF developed RFC 2196 provides a general and broad overview of information security including network security, incident response, or security policies. IETF Security Area Working Groups include: IP Security Maintenance and Extensions; Kitten (GSS-API Next Generation); Managed Incident Lightweight Exchange; Network Endpoint Assessment; Open Authentication; and Transport Layer Security.

ISA/IEC-62443 standards series define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

The IEEE standard, 802.11i-2004, implemented as Wi-Fi Protected Access II (WPA2), specifies security mechanisms for wireless networks. New versions of the IEEE 802.11 were published in 1999, 2007, and 2012. The next version is expected in 2016.

“Standards Being Developed” mostly appears in Table 1 for this core area.

Security Automation and Continuous Monitoring (SACM) While higher level standards for security automation and continuous monitoring are available and low-level specifications and implementations are in use, they require maturation and shepherding through international standards developing organizations.

Existing standards include a large body of work under ISO/IEC, IETF, and industry-led efforts (e.g., Cloud Security Alliance, HITRUST, NERC CIP) related to asset, configuration, and vulnerability management -- the underpinning of a continuous monitoring capability. Emerging standards include those being developed by the IETF Security Automation and Continuous Monitoring Working Group. Therefore, “Standards Being Developed” or “New Standards Needed” appears in Table 1 for this core area.

Supply Chain Risk Management (SCRM) There are two high-level SCRM standards available: the Open Group standard is focused on IT providers (not the acquirer) and the JTC1 standard, which is very general. However, in a couple of cases, standards developers are focused on SCRM for specific applications, such as by JTC1 for Cloud Computing and ISO TC 65 for ICS. While any organization and any application could use these higher level standards, more specific ones are more appropriate. This is why "New Standards Needed" appears in Table 1 for this core area.

Software Assurance It is important to have in place software assurance standards that provide assurance over the full lifecycle of software. For deployed software the ISO/IEC 19770-2 software identification (SWID) tagging standard, produced by JTC1 SC7, can be used to identify software, measure the integrity of software distributions and installations, and to detect and manage missing software patches. This together with source code and binary analysis techniques can provide improved software assurance for a number of deployed software scenarios that cross all of the key IT application areas. Further work is needed to either apply this existing standard to Cloud deployments or to identify additional approaches that address software and service deployments in Cloud scenarios.

System Security Engineering Relevant international standards are:

- ISO/IEC 21827:2008 specifies the Systems Security Engineering - Capability Maturity Model® (SSE-CMM®), which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering.

- The ISA/IEC-62443 standards series define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

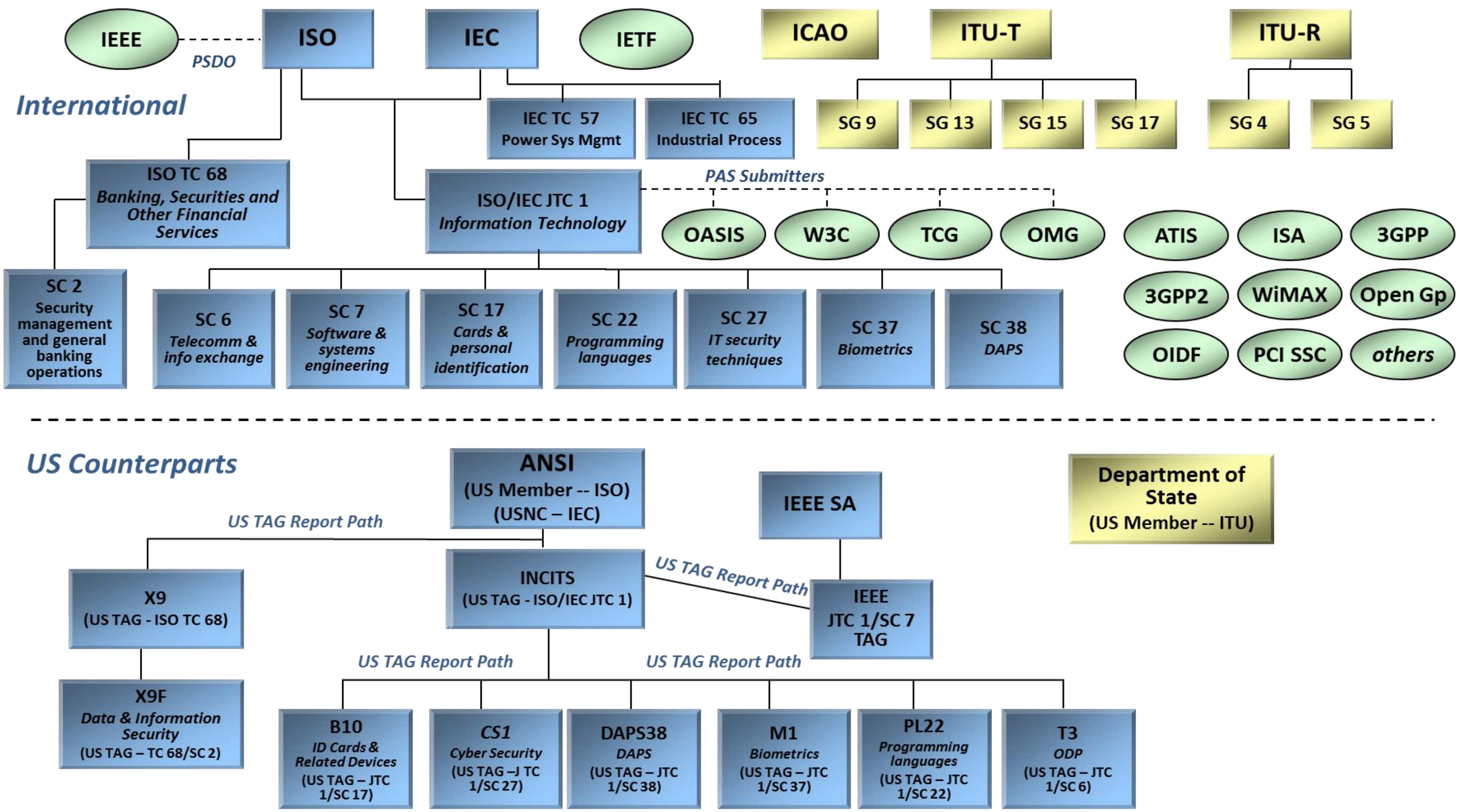
Further high level and application-specific standards work is needed for Systems Security Engineering.

6 Standards Developing Organizations (SDOs)

Worldwide, there are over 200 SDOs developing IT and ICS relevant standards.[6] Among those, there are dozens of SDOs developing cybersecurity standards, and yet fewer SDOs may be developing international standards.

However, these SDOs have many hundreds of cybersecurity standards projects under maintenance or development. Many of these standards are interdependent with each other. Therefore, in order to support overall cybersecurity, it is necessary to maintain consistency and interoperation with other standards from additional SDOs. Figure 1 illustrates some of the key cybersecurity SDOs and, where applicable, the U.S. national counterpart organizations.

[6] CEN Survey of ICT Standards Fora and Consortia; European Committee for Standardization, July 12, 2010



Key: PSDO = Partner Standards Development Organization; PAS = Publicly Available Specification; [blue box] = private sector, national member-based international standards body; [yellow box] = UN agency, member state-based international standards body ; [green oval] = international standards developer (e.g., consortium; industry association)

Figure 1 Examples of Key Cybersecurity SDOs

Annex E provides a matrix of key SDOs directly involved in cybersecurity. A brief description of these SDOs follows.

3GPP The 3rd Generation Partnership Project (3GPP) is a collaboration among groups of telecommunications associations established in December 1998, to make a globally applicable third generation (3G) mobile phone system specification within the scope of the International Mobile Telecommunications-2000 project of the ITU. 3GPP specifications are based on evolved Global System for Mobile Communications (GSM) specifications. 3GPP standardization encompasses Radio, Core Network and Service architecture. The groups are the European Telecommunications Standards Institute, Association of Radio Industries and Businesses/Telecommunication Technology Committee (ARIB/TTC) (Japan), China Communications Standards Association, Alliance for Telecommunications Industry Solutions (North America) and Telecommunications Technology Association (South Korea).

3GPP2 The Third Generation Partnership Project 2 (3GPP2) is a collaborative third generation (3G) telecommunications specifications-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 (ANSI: American National Standards Institute; TIA: Telecommunications Industry Association; EIA: Electronic Industries Alliance); Cellular Radiotelecommunication Intersystem Operations network evolution to 3G; and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). The ATIS Cloud Services Forum (CSF) is working to ensure that cloud services – as offered by service providers – are quickly operationalized to facilitate the delivery of interoperable, secure, and managed services. Current priorities include inter-carrier telepresence, content distribution network interconnection, cloud services framework, virtual desktop, virtual private network, and development of a cloud services checklist for onboarding.

IEC TC 57 The International Electrotechnical Commission (IEC), Technical Committee 57, Power systems management and associated information exchange, prepares international standards for power systems control equipment and systems including Energy Management Systems, SCADA, distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. IEC TC 57 Working Group (WG) 15 develops international standards addressing data and communications security for power systems.

IEC TC 65 The International Electrotechnical Commission (IEC), Technical Committee 65, Industrial process measurement, control and automation, prepares international standards for systems and elements used for industrial process measurement, control and automation. TC 65 coordinates standardization activities which affect integration of components and functions into such systems including safety and security aspects. This work of standardization is to be carried out in the international fields for equipment and systems.

IEEE The IEEE Standards Association (IEEE-SA) coordinates the efforts of experts throughout the IEEE in the development of standards such as key standards in the areas of computers, power and healthcare, and has 20,000 plus participants worldwide, including individuals in corporations, organizations, universities, and government agencies. An example IEEE of cybersecurity standards is the wireless local area network (WLAN) computer communication security standards (e.g., IEEE 802.11 series).

IETF The Internet Engineering Task Force (IETF) issues the standards and protocols used to protect the Internet and enable global electronic commerce. The IETF develops cybersecurity standards for the Internet. The wiki for the security area provides further details: <https://trac.tools.ietf.org/area/sec/trac/wiki>.

ISA The International Society of Automation (ISA) develops standards for automation and industrial control systems. Since 1949, over 150 standards have been developed by over 4,000 industry experts around the world. The ISA Standards Committee, ISA99, Industrial Automation and Control System Security, is developing a multipart standard for security for industrial automation and control systems. A sister committee is ISA100, Wireless Systems for Automation.

ISO/IEC JTC 1 The International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1), Information Technology, develops IT standards. ISO and IEC are private sector SDOs. In 1987, ISO and IEC established a joint Technical Committee by combining existing IT standards groups within ISO and IEC under a new joint Technical Committee, JTC 1. JTC 1 members are National Standards Bodies of different countries. Presently, there are 66 members. Approximately 2100 technical experts from around the world work within JTC 1. There are presently 18 JTC 1 Subcommittees (SCs) in which most of JTC 1 standards projects are being developed.

JTC 1 SC 27 (IT Security Techniques) is the one JTC 1 SC that is completely focused on cybersecurity standardization. Many other JTC 1 SCs are directly involved in specific standards critical to cybersecurity, including SC 6 (public key infrastructure [PKI] certificates), SC 7 (software and systems engineering), SC 17 (identification cards and related devices), SC 22 (programming languages, software environments and system software interfaces), and SC 37 (biometrics). In October 2009, JTC 1 established a new SC 38 for standardization in the areas of web services, Service Oriented Architecture (SOA), and cloud computing. SC 38 may also have specific cybersecurity standards projects in the near future.

ISO TC 68 The International Organization for Standardization Technical Committee 68 (ISO TC 68), Financial Services, develops standards in the field of banking, securities and other financial services. ISO TC 68 Subcommittee 2 (SC 2) develops international standards on security management and techniques applicable to general banking operations such as public key management and encryption algorithms.

ITU The International Telecommunication Union (ITU) is a treaty-based organization which was established in 1865. The ITU is based in Geneva, Switzerland, and its membership includes 191 Member States and more than 700 Sector Members and Associates. It has three sectors, the Radiocommunication (ITU-R), Telecommunication (ITU-T) and Development (ITU-D). Two of these sectors (ITU-R and ITU-T) develop cybersecurity standards. Of the two sectors, the ITU-T develops by far the most cybersecurity standards.

ITU-R The ITU Radiocommunication Sector (ITU-R) is responsible for radio communication. Its role is to manage the international radio-frequency spectrum and satellite orbit resources and to develop standards for radiocommunications systems with the objective of ensuring the effective use of the spectrum. ITU-R Study Groups involved in standards critical to cybersecurity include SG-4 (Satellite Services) and SG-5 (Terrestrial Services).

ITU-T The ITU Telecommunication Standardization Sector (ITU-T) develops standards for the telecommunications infrastructure including voice, data, and video. ITU-T Study Groups involved in standards critical to cybersecurity include SG-9 (Cable Systems); SG-13 (Next Generation Networks); and SG-17 (Network Security).

OASIS The Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit consortium that develops open standards for the global information society. The consortium produces Web services standards along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.

OIDF The OpenID Foundation is a non-profit international standardization organization of individuals and companies that is enabling, promoting and protecting OpenID technologies. Formed in June 2007, the foundation serves as a public trust organization representing the open community of developers, vendors, and users. OIDF assists the community by providing needed infrastructure and help in promoting and supporting expanded adoption of OpenID.

PCI SSC The Payment Card Industry Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.

TCG The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms. TCG has approximately 100 members from across the computing industry, including component vendors, software developers, systems vendors and network and infrastructure companies.

W3C The World Wide Web Consortium (W3C) is a non-incorporated international community of 334 Member organizations that develops standards in support of Web technologies. The W3C work in the area of cybersecurity standards includes secure transferring data from one domain to another domain or between applications with well-defined document authentication. XML Encryption and XML Signature are key pieces of the XML security stack.

WiMAX Forum The WiMAX Forum is an industry-led, not-for-profit organization formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI (European Telecommunications Standards Institute) HiperMAN standard.

IT Supply Chain Risk Management (SCRM) Standards

Figure 2 illustrates a 2009 review of standards activities involved in IT Supply Chain Risk Management (SCRM), which to a great extent covers the cybersecurity standards landscape. Figure 2 is based on ISO/IEC JTC 1 SC 7 (System and Software Engineering) and ISO/IEC JTC 1 SC 27 (IT Security Techniques) portfolios and lists of liaisons, as well as additional U.S. government and industry players involved in IT SCRM. It is presented here to illustrate the complexity of the landscape and the need to be involved in multiple standards bodies to be effective.

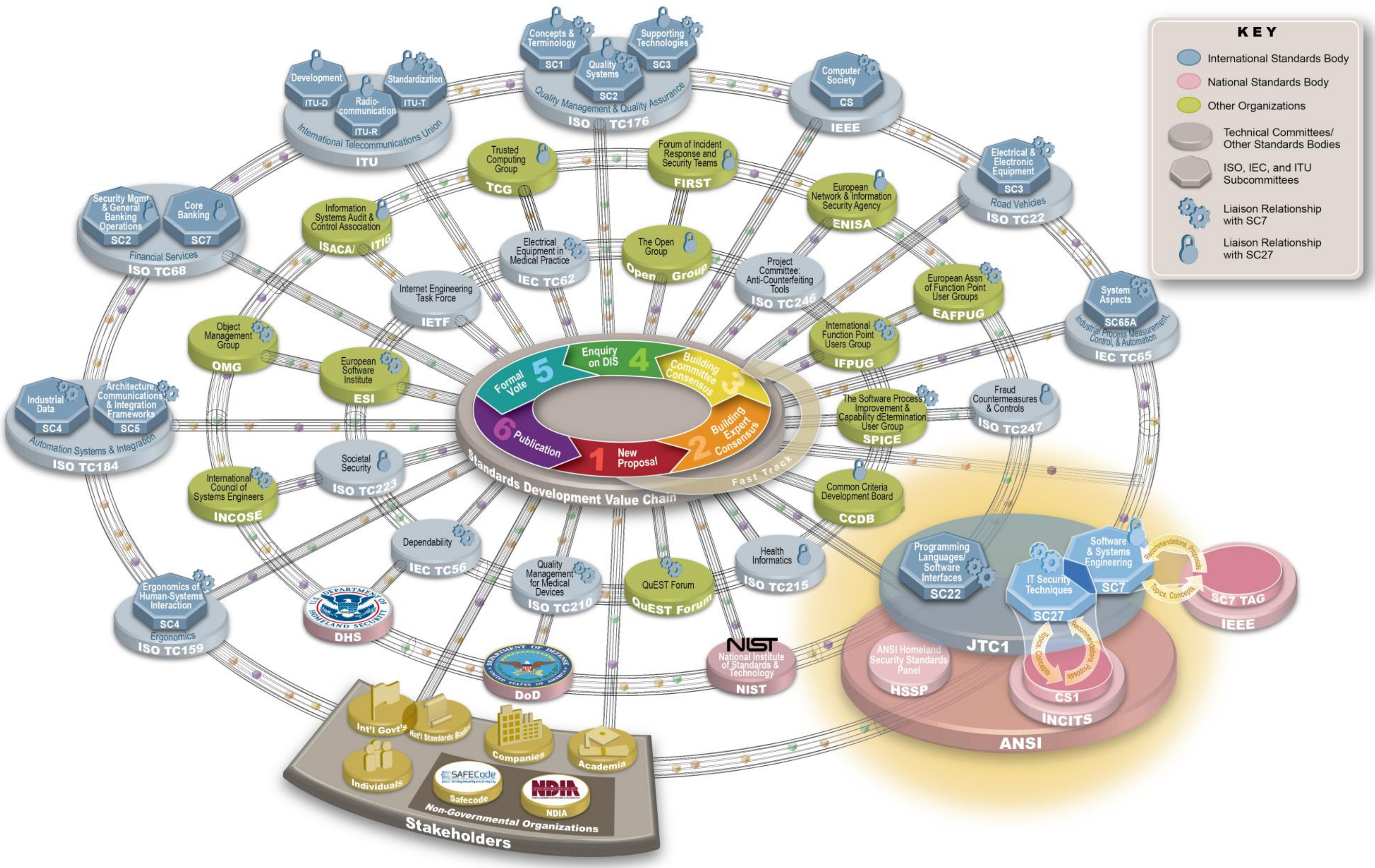


Figure 2 Standards Landscape for IT Supply Chain Risk Management (SCRM)

7 IT Standards Development

An SDO typically manages its portfolio of standards through a project management system, which facilitates active participation by technical experts and development of technically sound standards. When a standards project is proposed and approved, the project is assigned to a technical development group and a project editor is appointed; the project editor serves as the key office and catalyst for the timely development of the standard and is responsible for meeting any target dates for revisions. Through negotiations, the disposition of the comments received on a draft standard is approved by the meeting participants. Based upon the approved disposition of comments, the project editor prepares the next version of the standard. There may be many iterations of this process before the draft standard is considered complete and technically sound.

Market forces typically drive standards development. Standards development may be anticipatory or reactionary (or somewhere in between) with respect to products or services entering the marketplace. Many SDOs insist upon two or more successful independent implementations of the requirements in a draft standard before final approval of the standard. Additionally, such implementation developers can be a source of valuable technical feedback during the standard's development. Another market factor is that standards may be developed in a regulated or unregulated environment.

Figure 3 is a high-level, functional conceptualization of how IT standards are developed and standards-based IT products, processes and services are deployed. Depending on whether the project is anticipatory or reactionary (or somewhere in between), many of these functions will occur somewhat concurrently. Some of these functions (i.e., product/process/service/test tools development; testing; and deployment) occur outside of the SDO process but provide valuable feedback to the SDO functions.

For an SDO to start developing a standard, the members of the relevant SDO technical committee need a clear and comprehensive set of requirements for the intended application(s). Base standards often contain options so that such standards can support various applications. Profiles[7] make various options in one or more base standards mandatory in order to support a specific application area. The SDO may also develop testing methodology standards that can be used by test tool developers to ensure that resulting test tools correctly ascertain if an IT product, process, or service meets the requirements of the base or profile standards.

In more reactionary standards development, the requirements for a standards project are based upon commercially available products, processes, and services. In more anticipatory standards development, provider and consumer use cases will drive the requirements. The development of the draft standard can require many iterations, especially for groundbreaking anticipatory standards development. Specific IT applications may require the profiling of options in the base standard to support the interoperability, security, etc. requirements of the application. The

[7] Profiles define conforming subsets or combinations of base standards used to provide specific functions. Profiles identify the use of particular options available in the base standards, and provide a basis for the development of uniform, internationally recognized, conformance tests. [ISO/IEC TR 10000-1:1998] See also Annex A (Terms and Definitions.)

development of a testing infrastructure provides valuable feedback for all other stages of the IT standards lifecycle.

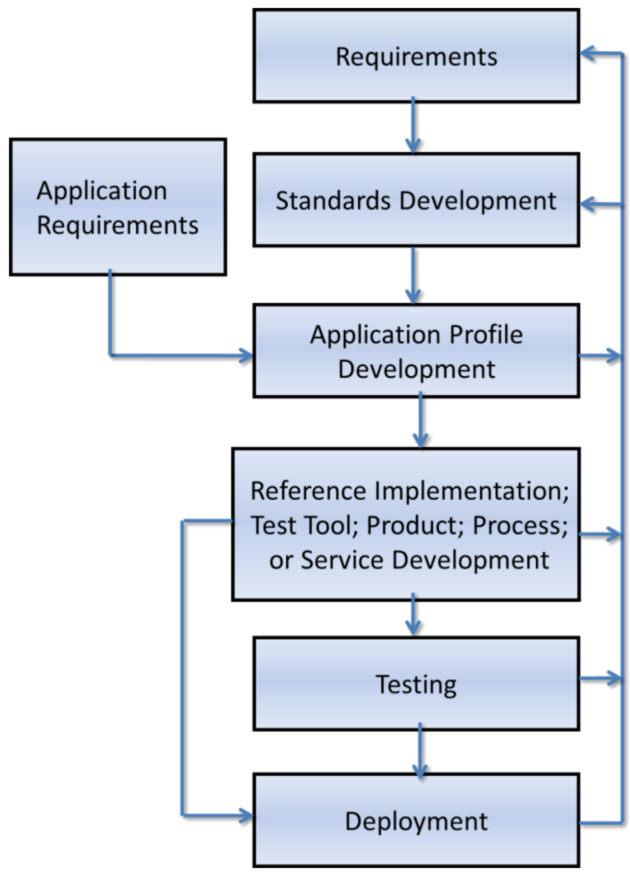


Figure 3 IT Standards Life Cycle

Many SDOs operate through a consensus process that is characterized by all or some of the following attributes: openness; transparency; balance; and due process or mechanisms for ensuring adherence to organizational procedures, including provision for appeals. Openness means that participation in standards development is open to all materially affected parties. Across the SDOs, there are different shades of openness, such as IETF's "anyone can participate" philosophy to ISO's limitation to member countries and recognized liaison organizations. Exposure of specifications to wide audiences during the development cycle can contribute to technical soundness. Transparency means that SDOs have clear and transparent processes for standards development to allow insight into the decision-making process and promote due process. Balance in an SDO is achieved by participation of vendors, system integrators, end users, consultants, academics, and others within the given technology area to ensure technical soundness and market relevance, and to ensure that to the extent possible no particular stakeholder group has undue influence in shaping the standard. Due process implies that mechanisms for ensuring adherence to organizational procedures, including provisions for appeals, are provided. Consensus requires that all views and objections be considered, and that an effort be made toward their resolution.

In the United States, the [National Cooperative Research Act of 1984] opened a new era where organizations could collaborate to carry out joint research and development ventures and not be deemed illegal per se under Federal antitrust laws or similar State laws. One result of this has been a rapid growth in IT consortia developing standards. In developing their standards, many of these consortia follow the above principles. However, consortia are also formed that are not open, with membership restricted to specific business allies. Consortia range from unincorporated affiliations of companies to incorporated entities with budgets, offices and paid staff. A consortium may exist to complete a specific standard, but others have a broader mission and develop multiple standards necessary to enable the evolution of a category of IT business services and products. An oft-cited advantage of consortia is speed in developing a specification, but speed is sometimes obtained by restricting the participation, which in turn may slow uptake of the developed specification.

Two case studies of SDOs are provided below to illustrate the diversity of standards development in the cybersecurity arena.

Case Study – IETF

The IETF is an open, bottom-up organization that develops Internet standards through the use of working groups. It has no formal membership, and final standards are published in the form of Requests for Comment (RFCs) (see http://www.ietf.org/rfc.html). All participants are volunteers and participate in working groups and/or the tri-annual public meetings and do not officially represent their home governments or organizations, but participate in an individual capacity. Accordingly, governments do not have any special status within the organization and standards generally become relevant through adoption, not government mandate.

The IETF's process provides participants with a great deal of autonomy to influence how the next generation Internet will grow and evolve, and what underlying principles the network will support. Within the IETF, there is an ongoing balance between protecting the core principles of the Internet (such as openness) and commercial profit interests. This has some effect on the types of standards that the Internet Engineering Steering Group (IESG) approves as final RFCs. Often, there are competing RFCs that may serve to address the same core problem. Yet, based on the IETF's "adoption" model, actual use of the standard dictates which standard will ultimately prevail.

Historically, U.S.-based industry has sent the largest contingent of participants to IETF meetings, but recently other countries have recognized the value of influencing the RFC development process and are sending more people to participate. Some countries are increasingly working in a more coordinated and unified manner with their industry members with clearly defined reporting structures and a defined set of joint goals. From a government and industry-relations perspective, some countries' regulatory and political regimes have certain advantages. For instance, the increase in globalization of the information and telecommunications technology industry makes it harder and harder to identify companies as U.S.-centric. Global companies have global loyalties and are often forced to respond to the regulatory and legal regimes of multiple nations. Further, within the United States the Internet industry remains unregulated, whereas in other regions of the world, IT companies may be partially state-owned, closely aligned with a local government regime, or closely regulated. Since the Internet was privatized in 1993, the USG has generally practiced a laissez faire approach to Internet standards development, allowing the private-sector to lead. Government experts participate in the IETF when they are working on a discrete need, but generally there has been little coordination of USG participants at IETF meetings to strategically track standards development that can impact national and economic security equities.

In many cases, companies would be inhibited from sharing certain information with one another due to protection of proprietary information and antitrust and other rules within the United States. However, there has also been limited outreach on the side of the government to industry partners to discuss ways of coordinating before meetings on areas that have the potential to impact national security equities. Participants, whether corporate or government, produce their own trip reports, but, these reports are not shared within USG or synthesized to create a holistic picture of all relevant activities and working groups at the IETF, which number in the hundreds. This lack of coordination means that participants act in isolation, and potentially against each other. Although this is appropriate in many commercial circumstances, there may be times when the USG may feel the need to leverage its U.S. industry counterparts within the IETF context to promote, shift, or eliminate a development that could have the potential to impact issues of national significance.

Case Study -- ISO

An ISO standard is expected to take two to four years from inception to publication primarily due to the time required to develop international consensus on positions. One method of developing an ISO standard is the use of the ISO five-step process that involves multiple draft reviews and requests comments from national bodies to advance drafts to the next formal stage of development. Advancing a standard from one formal stage to another requires an international ballot, voted on by each national body. With the votes, national bodies submit comments on the content, suggestions for improvement, and explanations for *no* votes. When a standard successfully advances through all required stages, it is published as an international standard.

ISO Technical Committees may also use the ISO "fast track" process, or other fast processes, for developing ISO standards. These processes can approve an ISO standard within 8 months. National Bodies or Category A liaison organizations of an ISO Technical Committee are permitted to submit candidate standards for ISO fast-track balloting. ISO/IEC JTC 1 has developed a Publicly Available Specification (PAS) process that allows consortia to fast process their PASs into ISO/IEC approved standards. Consortia, such as OASIS, TCG, the Open Group, the Object Management Group (OMG), and EUROPAY, have used the JTC 1 PAS process to quickly approve over 40 PASs as ISO/IEC standards.[8]

[8] ISO/IEC JTC1 PAS Submitters; International Organization for Standardization

8 Accelerating IT Standards Development

Assuming that the interagency determines that accelerating the development of a particular standard would be desirable, the ability of an SDO to expedite IT standards development would be related to several factors, including:

A. the level of effort expended by the participants;
B. the level of technical and "political" difficulty (see below) in developing the standard; and
C. the effectiveness of the consensus process being followed.

The development of a consensus IT standard may involve trade-offs among several attributes, such as speed, consensus, and quality, and it can require many iterations before there is a technically sound and comprehensive final draft. The process can be time consuming, especially if the consensus group meets only a few times a year. When a standards project is of high priority to a Federal agency or agencies, there are several factors discussed below that may need to be addressed in order to accelerate a standard's development without sacrificing quality.

A. Level of Effort

The technical expertise and resources provided for a particular IT standards development project are driven by market forces and deadlines. For most standards projects, participating IT experts from various stakeholder organizations typically allocate only a fraction of their time to standards development. In such situations, standards meetings of only a few days' duration occur a few times a year. For other standards projects, time-to-market pressures and/or mandated deadlines can lead to technical experts working essentially full time for several months to complete a standard.

Examples: FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors (2005) and the Registered Traveler Interoperability Consortium (RTIC) Specification (2006) are examples of high levels of effort that resulted in standards being developed within six months. Such timing was possible because of the resources dedicated to the work and the fact that both of these standards profiled already available base standards.

Example: The U.S. High Definition Television (HDTV) standard was developed quickly by industry in the early 1990s. The impetus for this rapid standards development was the declaration by the Federal Communications Commission (FCC) that industry had a specific deadline to produce such a standard and demonstrate its viability or the FCC would develop the standard. Industry quickly collaborated to develop the digital specification, established a testing facility, and demonstrated interoperable digital technology. Of course, deployment of the new HDTV digital infrastructure took over fifteen years, with the older analog TV broadcasts ending on June 12, 2009.

B. Level of Difficulty

The difficulty in developing an IT standard includes technical and political issues. Technical challenges range from the difficulty of developing a sound test method for standard requirement(s) to the need to develop thousands of test cases necessary for rigorous and comprehensive testing of complying implementations. Political difficulties include: vendor resistance to commoditizing an IT market through standardization, turf fights between standards developers, and the individual egos of the participants. While ensuring that all the important parties are in agreement before a project begins can greatly accelerate the standardization process, competitive standards solutions pushed by different industry alliances make such advance agreements problematic.

Example: Extensive peer reviewed testing is necessary before standardizing encryption algorithms because no definitive technical approach is known for ensuring an algorithm has no exploitable security flaw. Starting in 1997, NIST's Information Technology Laboratory (ITL) led a worldwide, multiyear project to find a replacement standard for the Data Encryption Standard (DES). The approaching end-of-life for DES, which was originally developed in the 1970s, was widely recognized due to steadily increasing computer processing power. NIST solicited candidate encryption algorithms and provided a forum for peer reviewed testing of the candidate algorithms. As a result of that extensive testing, an algorithm was selected and FIPS 197, Advanced Encryption Standard (AES), was approved in November 2001. NIST also developed a conformance testing program for the AES. AES was subsequently incorporated into ISO/IEC 18033-3:2005 Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers.

Example: NIST led the test tool development for the Portable Operating System Interface (POSIX) standard developed by the IEEE. Working in support of the IEEE POSIX standards project, NIST staff and industry guest researchers developed about 100,000 test assertions, which served as the basis for producing the executable test code of the POSIX test tool. This test assertion/test code development took about three years.

Example: Business alliances are often formed to promote competitive solutions. Such competition is reflected is standardization. The completion of the standards can be delayed by such competition and the market acceptance of the final standards is slowed. Examples of format wars include the video tape formats (VHS versus Betamax) introduced in the 1970s, the micro flexible disks (e.g., 90 mm) introduced in the 1980s and more recently the rival high definition DVD formats (HD DVD versus Blu-ray Disc).

C. Effectiveness of Consensus Standards Development Processes

Many SDOs are in competition for new IT standards projects. As a result of this competitive environment, over the last 20 years many SDOs have streamlined their consensus development processes and added fast track processes to their repertoires. The effectiveness of standards processes, streamlined or other, also depends greatly upon the availability of experienced, competent leadership and administration that ensure that best practices are followed.

Example: Starting in 1997, the Industry Usability Reporting Project (IUSR) developed a software usability specification and conducted pilot testing. In less than five months, using the INCITS (International Committee for Information Technology Standards) fast track process, the consortium's specification was approved in American National Standard INCITS 354-2001, Information Technology – Common Industry Format for Usability Test Reports. In less than six months, using the JTC 1 fast track process, INCITS 354 was approved as International Standard 25062:2005, Software Engineering- Software Quality and Requirements Evaluation - Common Industry Format for Usability Test Reports. The multi-year delay between the national and international versions was largely due to a turf fight in the United States on where to fast track internationally.

Example: The BioAPI Consortium submitted its BioAPI specification to INCITS in September 2001. INCITS 358:2002 - American National Standard for Information Technology – The BioAPI Specification was approved in February 2002. This standard was submitted to ISO/IEC JTC 1/SC 37 for fast processing in 2003. It was approved as ISO/IEC 19784-1:2006 Information technology - Biometric application programming interface – Part 1: BioAPI specification. The SC 37 "fast processing" was slowed by the urge of the international technical experts to improve the standard, which in fact they did, but adding years to the development time.

9 Ongoing Issues in IT Standards Development

The following issues illustrate some of the factors that affect IT standards development. Such issues are likely to be ongoing, with no prospect for easy resolution, and therefore are expected to be part of the long term environment of IT standards development.

IT Standards and Public Policy

An issue that has become increasingly relevant to U.S. interests is the policy direction some SDOs are taking when drafting "technical" standards. Over the past several years, certain countries have begun to "forum shop" their specific public policy or trade interests and issues and have found acceptance in certain SDOs. Although the USG and the U.S. private sector have vocally opposed SDO attempts at drafting public policy through the creation of technical standards, many parties see opportunities in the drafting process to encourage the adoption of policies that reflect their particular agendas. Without a strategy in place, this can be challenging to combat because many of the U.S. representatives to these committees are technical experts not involved in public policy debates. Based upon a U.S. contribution on this issue, ISO and IEC have re-stated their commitment to develop international standards that are market relevant, meeting the needs and concerns of all relevant stakeholders including public authorities where appropriate, without seeking to establish, drive or motivate public policy, regulations, or social and political agendas.[9]

[9] ISO/IEC JTC 1 N 9623, Principles for Developing ISO and IEC Standards Related to or Supporting Public Policy Initiatives,

Open IT Standards

Open IT standards facilitate the exchange of data and interoperability with other IT systems, perhaps of different design or manufacture, by publicly defining requirements such as for interoperating processes, data formats (e.g., binary, ASCII, XML), interfaces (e.g., physical, software, logical), and protocols (e.g., syntactic and semantic rules for communication functions).

Definitions for open standards vary within the IT industry. For various IT product, process and service markets, IT companies break into factions about the preferred definition of "open" standards based upon their market shares and whether that market sector presently depends upon open or proprietary standards. The only common denominator for "open" standard among all of these factions appears to be that the standard is publicly available, whether for free or for a cost.

A major issue for IT companies is if the standard requires reading on a patent to implement (a standard essential patent, or SEP). The SEP issue consists of two parts. The first is whether the SEP is required to be made available by a licensor on a Royalty Free (RF) or Reasonable and Non Discriminatory (RAND) basis; another option is RANDZ (Reasonable Non-discriminatory and Zero-cost). The second is whether the SDO requires early notification of potential SEPs by patent holders while a standards project is under development or if notification by a patent holder is voluntary.

The World Wide Web Consortium (W3C) now insists that all of its standards be implementable RF. The ISO/IEC and ITU-T require that their standards be implementable RF or RAND. The IETF traditionally favors technologies that are RF, but does not impose strict requirements. However, the IETF requires "immediate" disclosure of patented technology or patent claims known to any participant (not just the patent holder), even if the technology was contributed to the project by another participant.

Differences between the U.S. and Other National/Regional Standards Systems

As discussed in the overview, the U.S. standards system differs significantly from the government-driven standards systems in many other countries and regions. Hundreds of SDOs -- most of which do not develop cybersecurity standards -- are domiciled within the United States. These organizations provide the infrastructure for the preparation of standards documents, and government personnel participate in SDO activities along with representatives from industry, academia, and other organizations and consumers. It is important to emphasize that these SDOs are primarily private-sector organizations and that the Federal government is simply one of many stakeholders and participants. The United States Standards Strategy, elaborated through a private-public partnership in 2005, outlines the contribution of private-sector led standards development to overall competition and innovation in the U.S. economy.

In many other standards systems, the government plays a larger role in standards development related activities. In such cases, these governments have more leverage to use standards as tools for competition and innovation policy." While U.S. Government agencies possess certain responsibilities related to standards, such as in the use of standards in regulation, procurement, or other activities, there is a much greater reliance in the United States than in the European Union or China on obtaining input from industry groups, consumers, and other interested parties in making decisions related to the technical content of standards and on allowing the private sector to drive standards development. By contrast, other governments have instituted top-down standards systems, which may involve governmental direction to stakeholders to develop particular standards, the provision of funding to national delegations, and hosting meetings.

10 How to Effectively Engage SDOs

"Laws, like sausages, cease to inspire respect in proportion as we know how they are made.[10]

Consensus among participants in various SDOs to approve standards usually requires more than a majority but less than unanimity. Where there is voting to establish consensus, it may be voting by all participants, by one vote per organization (e.g., national body, company) or by weighted organizational voting. In all such scenarios, a Federal agency, or even several Federal agencies, will typically not have sufficient voice to gain approval for their technical contributions without agreement by other SDO participants. This requires effective representation and negotiation by the agency participants over many meeting cycles.

Effective negotiation in international standards development requires not just technical expertise, but a thorough knowledge of the SDO's standards development process and policies. Standards participation also requires knowledge of, and relationships with, the individual players, including both the leadership of the bodies and the technical experts involved – and for international fora, understanding of the culture of the fora and its participants. Awareness of the relevant IT market and associated market politics, which drive the motivations of the other participants, is likewise essential.

Continuity in participation is crucial to success. Participants must attend the meetings regularly over a period of one or more years and have established relationships with the other participants to facilitate necessary progress in moving the agenda forward and ensuring that the draft standards are technically sound and meet USG needs. It is important to understand and take advantage of the fact that negotiations occur before, after, during and in between the formal meeting sessions. In large standards projects, it is often difficult to draw participants' attention to the specific needs of particular parties unless their representatives have obtained the respect of other participants through continuous attendance, thoughtful participation, and contribution to the needs of the project itself.

Effective leadership in SDOs promotes timely development of technically sound standards. It is in the best interest of Federal agencies to support qualified Federal representatives (including contracted technical experts) in SDO leadership positions. Candidates for such leadership positions should be both technically knowledgeable and thoroughly familiar with the SDO's development processes and policies. Key SDO leadership positions include chairing or convening groups, providing the administrative/secretariat functions for groups, and serving as the project editor for a specific standards development project.

---

[10] See The Daily Cleveland Herald, Mar. 29, 1869, quoting the lawyer-poet John Godfrey Saxe.

In addition to effective participation and leadership by Federal agency representatives, Federal agencies, consistent with agency missions, need to coordinate their positions. Office of Management and Budget (OMB) Circular A-119 [Section 15. b. (3)] emphasizes the need for interagency coordination and cooperation in voluntary standards development:

> "Ensuring, when two or more agencies participate in a given voluntary consensus standards activity, that they coordinate their views on matters of paramount importance so as to present, whenever feasible, a single, unified position and, where not feasible, a mutual recognition of differences."

The USG also needs to effectively engage with U.S. stakeholders. There are several methods agencies can use to engage and coordinate with stakeholders. Agencies may choose to establish external advisory committees per the Federal Advisory Committee Act (FACA), seek input using Federal Register Notice solicitations, use specific statutory or regulatory authority to create a forum for obtaining input, or use some other method that provides all potential stakeholders an equal opportunity to provide input and share their perspectives.

Following are several examples of USG engagement and coordination that may be relevant for this space:

- The Department of Homeland Security has established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments. The CIPAC represents a partnership between government and critical infrastructure/key resource (CIKR) owners and operators and provides a forum to engage in a broad spectrum of activities to support and coordinate critical infrastructure protection.

- Under the Energy and Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) was responsible for coordinating the development and publishing of a framework, including protocols and model standards, to achieve secure interoperability of Smart Grid devices and systems, with input and cooperation from other Federal and State agencies and interested private sector entities. In April 2013, the Smart Grid Interoperability Panel (SGIP) fully transitioned to a non-profit private-public partnership organization, SGIP 2.0, Inc., supported by industry stakeholder funding and funding provided through a cooperative agreement with NIST. NIST continues an active role in the SGIP. Current news and member information now resides at SGIP.org. The SGIP reviews use cases, identifies requirements and architectural reference models, coordinates and accelerates Smart Grid testing and certification, and proposes action plans for achieving these goals. The SGIP does not write standards, but serves as a forum to coordinate the development of standards and specifications by many SDOs.

- 22 U.S.C. §2707 provides that the Secretary of State is responsible for formulation, coordination, and oversight of foreign policy related to international communications and information policy. The State Department uses a Federal Advisory Committee to obtain the views of the private sector in developing U.S. positions with respect to cybersecurity standards that are being developed at the ITU.

- The Department of Commerce and USTR co-administer sixteen Industry Trade Advisory Committees (ITACs), an ITAC Committee of Chairs, and more than 300+ trade advisors, who provide detailed policy and technical advice and recommendations to the Secretary of Commerce and the USTR regarding trade barriers, negotiation of trade agreements, and implementation of existing trade agreements affecting industry sectors; and perform other advisory functions relevant to U.S. trade policy matters.

It is important to prioritize resources and engagement for maximum impact with various SDOs. To do this requires additional coordination, organizational buy-in, allocating budget to participate in standards over the potentially lengthy process of standards development, and holding lower-level technical personnel accountable to participate in SDOs. The number of cybersecurity standards projects is substantial; therefore an engagement model is required to ensure that the U.S. government is able to dynamically engage at the right level when necessary.

The following four categories characterize the potential levels of engagement and resource planning needs that the interagency may determine is warranted for particular standards development projects:

Lead – in addition to monitoring and influencing (see below) provide resources to edit strategically important standards; chair committees, study groups, and other meetings; lead delegations; comment and provide text contributions to strategically important standards. This requires technology expertise in the areas of interest, as well as process leadership, knowledge of SDO procedures and stakeholders, and the ability to actively represent national position/requirements to the external standards activity.

Influence – in addition to monitoring (see below), provide resources to comment and provide text contributions to strategically important standards; work with industry and international players interested in the same subject and exert influence through formal and informal discussions and expertise. This requires technology expertise in the areas of interest and the ability to actively represent national position/requirements to the international standards activity.

Monitor - monitor programs of work and emerging and evolving standards produced by the SDOs of interest; develop an understanding of and relationships with the key players to allow for greater engagement when appropriate. Report on the progress of SDO program of work and on the standards of interest. This requires technology expertise in the areas of interest.

Participating - in limited specific activities is following, contributing to, and/or leading a specific standards effort for a select activity(s) specific to unique needs or interests.

All of these options include having USG participants function in these capacities, based on expertise, relationships, and knowledge of specific SDO processes.

Annex A – Terms and Definitions

For the purposes of this document, the terms and definitions in this Annex apply. Note that, in some instances, more than one definition is provided to highlight that authoritative sources may develop different explanations for the same term.

Base Standards[11] define fundamentals and generalized procedures. They provide an infrastructure that can be used by a variety of applications, each of which can make its own selection from the options offered by them.

Conformity Assessment[12] is activity that provides demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.

Cyber refers to both information and communications networks. [SOURCE: This report]

Cybersecurity is defined as the prevention of damage to, unauthorized use of, exploitation of, and -- if needed -- the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems. [SOURCE: This report]

Cyberspace[13] is the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

Industrial Control System (ICS)[14] is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures.

Information Technology (IT)[15] The art and applied sciences that deal with data and information. Examples are capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage, and retrieval of data and information.

Information and Communications Technologies (ICT) encompasses all technologies for the capture, storage, retrieval, processing, display, representation, organization, management, security, transfer, and interchange of data and information. [SOURCE: This report]

---

[11] ISO/IEC TR 10000-1:1998, Information technology -- Framework and taxonomy of International Standardized Profiles -- Part 1: General principles and documentation framework

[12] ISO/IEC 17000:2004, Conformity assessment -- Vocabulary and general principles

[13] Draft ISO/IEC 27032, Information Technology – IT Security Techniques – Guidelines for Cybersecurity

[14] NIST Special Publication 800-82, Revision 2 Initial Public Draft, Guide to Industrial Control Systems (ICS) Security.

[15] American National Standard Dictionary of Information Technology (ANSDIT)

Profiles[16] define conforming subsets or combinations of base standards used to provide specific functions. Profiles identify the use of particular options available in the base standards, and provide a basis for the development of uniform, internationally recognized, conformance tests.

A **Qualified Products List**[17] is a list of products that have met the qualification requirements stated in the applicable specification, including appropriate product identification and test or qualification reference number, with the name and plant address of the manufacturer and distributor, as applicable.

Reference implementation is the implementation of a standard to be used as a definitive interpretation for the requirements in that standard. Reference implementations can serve many purposes. They can be used to verify that the standard is implementable, validate conformance test tools, and support interoperability testing among other implementations. A reference implementation may or may not have the quality of a commercial product or service that implements the standard. [SOURCE: This report]

Resilience[18] is the ability to reduce the magnitude and/or duration of disruptive events to critical infrastructure. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

Resilience[19] can also be defined as the adaptive capability of an organization in a complex and changing environment.

Security[20] refers to information security. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

A. **Integrity**, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
B. **Confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
C. **Availability**, which means ensuring timely and reliable access to and use of information.

[16] ISO/IEC TR 10000-1:1998, Information technology -- Framework and taxonomy of International Standardized Profiles -- Part 1: General principles and documentation framework

[17] 41 CFR 101-29.207 [Title 41 Public Contracts and Property Management; Subtitle C Federal Property Management Regulations System; Chapter 101 Federal Property Management Regulations; Subchapter E Supply and Procurement; Part 101-29 Federal Product Descriptions]

[18] CRITICAL INFRASTRUCTURE RESILIENCE FINAL REPORT AND RECOMMENDATIONS, NATIONAL INFRASTRUCTURE ADVISORY COUNCIL, SEPTEMBER 8, 2009

[19] ASIS International, ASIS SPC.1-2009, American National Standard, Organizational Resilience: Security, Preparedness, and Continuity Management System – Requirements with Guidance for Use.

[20] Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA)

Security[21] may also be defined as the preservation of confidentiality, integrity and availability of information. NOTE In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be relevant.

A. **Integrity**, property of protecting the accuracy and completeness of assets;
B. **Confidentiality**, property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
C. **Availability**, property of being accessible and usable upon demand by an authorized entity.

Software Assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions as intended by the purchaser or user. [SOURCE: This report]

Standard[22] is a document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note: Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.

Standard can also be defined as a document that may provide the requirements for: a product, process or service; a management or engineering process; or a testing methodology. An example of a product standard is the multipart ISO/IEC 24727, *Integrated circuit card programming interfaces*. An example of a management process standard is the ISO/IEC 27000, *Information security management systems*, family of standards. An example of an engineering process standard is ISO/IEC 15288, System life cycle processes. An example of a testing methodology standard is the multipart ISO/IEC 19795, *Biometric Performance Testing and Reporting*. [SOURCE: This report]

Standards Developing Organization (SDO) is any organization that develops and approves standards using various methods to establish consensus among its participants. Such organizations may be: accredited, such as ANSI-accredited IEEE; international treaty based, such as the ITU-T; private sector based, such as ISO/IEC; an international consortium, such as OASIS or IETF; or a government agency. [SOURCE: This report]

Supply Chain Risk Management (SCRM) is the implementation of processes, tools or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. [SOURCE: This report]

---

[21] ISO/IEC 27000:2009, Information Technology – IT Security Techniques – Information Security Management Systems – Overview and Vocabulary.
[22] ISO/IEC Guide 2:2004, Standardization and related activities - General Vocabulary, definition 3.2.

Test Tools are a means of testing to confirm that an IT product, process, or service conforms to the requirements of a standard or standards. Examples of test tools are executable test code or reference data. [SOURCE: This report]

Annex B – Conformity Assessment (CA)[23]

Conformity assessment enables buyers, sellers, consumers, and regulators to have confidence that products sourced in global market meet specific requirements. It is the demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.

Conformity assessment procedures provide a means of ensuring that the products, services, systems, persons, or bodies have certain required characteristics, and that these characteristics are consistent from product to product, service to service, system to system, etc. Conformity assessment can include: supplier's declaration of conformity, sampling and testing, inspection, certification, management system assessment and registration, the accreditation of the competence of those activities, and recognition of an accreditation program's capability.

Standards are interwoven into all aspects of these activities and can have a major impact on the outcome of a conformity assessment scheme or program. Conformity assessment activities form a vital link between standards (which define necessary characteristics or requirements) and the products themselves. Together standards and conformity assessment activities impact almost every aspect of life in the United States.

A specific conformity assessment scheme or program may include one or more conformity assessment activities. While each of these activities is a distinct operation, they are closely interrelated.

Conformity assessment activities can be performed by many types of organizations or individuals. Conformity assessment can be conducted by: (1) a first party, which is generally the supplier or manufacturer; (2) a second party, which is generally the purchaser or user of the product; (3) a third party, which is an independent entity that is generally distinct from the first or second party and has no interest in transactions between the two parties; and (4) the government, which has a unique role in conformity assessment activities related to regulatory requirements.

Terminology for conformity assessment is found in standard ISO/IEC 17000.

Types of Conformity Assessment[24]

Conformity assessment activities can be performed by many types of organizations or individuals. It can be conducted by:

1. ***first party***, which is generally the supplier or manufacturer;
2. ***second party***, which is generally the purchaser or user of the product;
3. ***third party***, which is an independent entity that is generally distinct from the first or second party and has no interest in transactions between the two parties; or

[23] See NIST Conformity Assessment Overview.
[24] See http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-208

4. ***the government***, which has a unique role in conformity assessment activities related to regulatory requirements. It should be noted that in the procurement area, the government acts as a second party.

The following are different types of conformity assessment activities that these organizations use to determine that products, services, systems, persons, or bodies meet the specified requirements. While each of these activities is a distinct operation, they are closely interrelated.

Supplier's Declaration of Conformity (1st party only)[25]

A Supplier's Declaration of Conformity (SDOC), sometimes called a Manufacturer's Declaration of Conformity or even (incorrectly) self-certification, is a first party assessment in which a supplier or manufacturer provides written assurance of conformity.
SDOC is generally used when:

- the risk associated with noncompliance is low;
- there are adequate penalties for placing noncompliant products on the market; and
- there are adequate mechanisms to remove noncompliant products from the market.

ISO/IEC standard 1750 Parts 1 and 2 define requirements for suppliers and manufacturers to meet when they make formal claims that products, services, systems, processes or materials conform to relevant standards, regulations or other specifications. The standard has two parts. Part 1 specifies the general requirements for an SDOC. Part 2 contains requirements for supporting documentation to substantiate an SDOC, such as testing carried out by the supplier or an independent body.

Sometimes the declaration takes the form of a separate document or label. The supplier makes such a declaration based on: (1) the manufacturer's confidence in the quality control system; or (2) the results of testing or inspection the manufacturer undertakes or authorizes others to undertake on his/her behalf. The manufacturer has the option of using an accredited laboratory or inspection body and indicating this on the declaration. However, this is not a requirement. The choice of where to test is left to the manufacturer. For regulatory purposes, authorities can ensure that the integrity of an SDOC is maintained by establishing requirements for who signs the declaration of conformity, requiring access to the declaration and/or compliance records, etc.

Reliance on an SDOC is considered to be a trade-friendly approach to conformity assurance. From a manufacturer's perspective, the SDOC allows flexibility in choosing where to have a product tested, reduces the uncertainty associated with mandatory testing by designated foreign laboratories, as well as generally reducing associated testing costs and time to market.

SDOC can also be a cost-saving and efficient tool for regulators to meet their legitimate policy objectives, such as ensuring protection of the environment or the health and safety of consumers. In addition, the SDOC is beneficial because there is no discrimination on the basis of the geographic location of a testing or other conformity assessment body -- in short, conformity is the responsibility of the supplier. Under such a system, the question of "portability" of

[25] See http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-208.

conformity assessment, or of the need to negotiate political agreements on mutual recognition, become moot.

In the United States, some regulatory agencies use SDOC for certain, but not all, equipment. For example, the U.S. Federal Communications Commission (FCC) has adopted a rule that permits recognition of SDOC for certain digital devices. For other equipment, such as personal computers and attachments thereto, the FCC allows the equipment declared compliant by the supplier, under a process called Declaration of Conformity, provided supporting test results are obtained from an accredited laboratory. This program benefits manufacturers in two ways: reducing costs and time to market while maintaining a high level of protection of health and safety.

Other U.S. regulatory agencies also rely on SDOC for technical regulations. For example, the U.S. Department of Transportation accepts SDOC from manufacturers or importers of motor vehicles and motor vehicle equipment. Under U.S. law, manufacturers are required to certify that their products comply with all applicable Federal Motor Vehicle Safety Standards (FMVSS). This certification is in the form of a permanent label affixed to the product. This label is required for all vehicles and equipment covered by the FMVSS and must be present if a vehicle or equipment covered by the FMVSS is to enter the United States.

While the SDOC can save costs, such an approach to conformity assurance may not always be appropriate, particularly where technical infrastructure is lacking or it would compromise health, safety or environmental protections.

Inspection (1st, 2nd or 3rd party)[26]

Inspection is defined in ISO/IEC 17000 as "examination of a product design, product, process or installation and determination of its conformity with specific requirements, or on the basis of professional judgment, with requirements."

Inspection can be performed by first, second or third parties. Generally, inspection systems only demonstrate conformity of the actual products inspected or a lot from which the inspected samples are drawn. Inspection is well-suited to product characteristics that can be readily measured and where production occurs in batches. The supplier can arrange for the inspection of a production batch when needed. However, for products in continuous production, the cost of having an inspector present during production may be restrictive.

Inspection is also used to ensure that component parts and materials have been installed correctly. This type of conformity assessment is often applied to structures that must meet regulatory requirements. The inspection may need to take place in phases based on the ability to inspect portions of the structure at certain phases of the construction. Second-party inspections are carried out by manufacturers on the suppliers of critical components and subassemblies that will go into their finished products. Many inspection programs use product markings such as the U.S. Department of Agriculture meat grades or certificates to attest to the conformity of inspected products. Inspection is also used as part of a more comprehensive conformity

[26] See http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-199.

assessment system. For example, inspection is often used in the surveillance activities of certification systems

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have published a standard for organizations that operate primarily as inspection bodies, ISO/IEC 17020:1998, general criteria for the operation of various types of bodies performing inspection, which is currently being revised.

Testing (1st, 2nd or 3rd party)[27]

ISO/IEC 1700 defines testing as the "determination of one or more characteristics of an object of conformity assessment, according to a procedure," also known as a test method. The objects of testing are generally selected using some form of sampling procedure or process. The sampling process should be selected in a manner that is designed to ensure the validity of the test results or data. If the test method is well written and the sampling process is adequate, the test data should comply with the test method's requirements for accuracy and variability.

Testing laboratories support billion dollar industries and affect the operation of U.S. and foreign industries and regulatory systems. Each day major corporate and regulatory decisions are made based on data produced by testing laboratories.

Test data are used in many tasks, including:

- Product design and research
- Quality control prior to acceptance of incoming materials/components, during production, and prior to shipment/sale
- Insurance underwriting
- Meeting contractual agreements
- Satisfying government regulatory requirements
- Certification and labeling
- Buyer protection and information
- Product comparisons
- Building and structure design, construction and related engineering tasks
- Medical and health services
- Environmental protection
- Product operation, maintenance and repair
- Legal proceedings
- Forensic work

Flawed test data can result in defective products capable of causing serious injury or harm to the user or the environment. Defective products (such as fire detection and mitigation equipment and systems, security alarms, aircraft, and autos) can also result in serious injury or death - not only to users, but also to unsuspecting bystanders.

[27] See http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-205.

Testing can be performed by laboratories differing widely in size, legal status, purpose, range of testing services offered, and technical competence. In the United States, they may be government regulatory laboratories, government research laboratories, or government-supported laboratories - at the federal, state or local levels. They can also be college/university laboratories, independent private sector laboratories, laboratories affiliated with or owned by industrial firms or industry associations, or manufacturers' in-house laboratories. Test laboratories can be for-profit or not-for-profit. Laboratories can operate facilities in one or multiple locations; and may even operate in multiple countries. Laboratories can offer only a limited range of testing services or services in many fields. In the United States, there are almost as many different types of laboratories as there are different types of users of the test data that the laboratories produce.

Accuracy (or bias) refers to the degree of departure of the test result from the "true value." For example, if a product is weighed and the result is 5.1 kg (when the actual weight is 5.0 kg), the test or measurement is inaccurate by.1 kg. The required degree of accuracy will depend on the characteristic being tested and the impact of test data accuracy on the ability of the product being tested to perform in an acceptable manner.

Variability (or precision) refers to the degree of difference between the results from several repetitions of the same test. For example, if that same product (weighing 5.0 kg) were measured three times and the weights were recorded as 5.1 kg, 4.9 kg, and 5.0 kg., these results vary less than if measurements for that product were 4.5 kg, 5.0 kg and 5.5 kg.

Variability can be further defined in terms of repeatability, which is a measure of the variation among the test results when the same or similar test is repeated within one laboratory. Reproducibility (or replicability) is a measure of variation of test results from similar tests conducted in different laboratories. Reproducibility can be a key concern in conformity assessment programs, which use multiple laboratories.

A low degree of accuracy or increased variability in test results may occur not only due to errors by the laboratory staff or defects in the test equipment, but may also arise from other factors, such as flaws or variables in the test method or in the sample selection process. As noted elsewhere, the selection of good test methods and the use of an acceptable sampling process are vital to the production of good test results. Because test results are a vital component of most conformity assessment programs, the use of good test data is essential for the credibility of any such program.

Standards organizations have long recognized the importance of laboratory competence. For example, ISO/IEC 17025, "General Requirements for the Competence of Testing and Calibration Laboratories," establishes general requirements for laboratory competence to conduct specific test or calibrations. The laboratory requirements set forth by this standard are both management and technical in nature. The compliance of a laboratory with ISO/IEC 17025 or its equivalent provides some assurance of the competence of that laboratory.

Certification (3rd party only)[28]

Many certification programs focus on product characteristics related to health, safety and protection of the environment. In addition, certification programs also focus on other product performance characteristics.

Certification systems are also used to enhance the purchaser's ability to compare product attributes, such as the usable volume of a refrigerator or grades of motor oil. In these cases the certification provides confidence that the rated volume or viscosity is based on testing and measurement in accordance with accepted standards. Still other programs certify that products actually come from a certain place, such as potatoes grown in Idaho. These types of certification programs are often developed by suppliers, or trade or professional organizations in response to a market need for reliable information on product characteristics.

ISO/IEC Guide 65, General requirements for bodies operating product certification systems, (to be replaced by ISO/IEC 17065) contains a set of general criteria for the operation of a certification program by a third party. This standard is used by many but not all certification programs.

A competently operated certification program can provide a valuable communication tool that can reduce the cost of exchanging information among sellers, buyers, and other interested parties. However, the quality of the information conveyed via a specific certification program depends on many factors. Users of certification results need to be educated on the details of the certification process to enable them to assess the value of certification information and to make intelligent choices regarding its usage.

Product Certification

Product certification programs can be voluntary or mandatory and they may be carried out by either private sector bodies or government agencies.

Certification has two essential characteristics. It is conducted by an independent third party and includes some form of surveillance activity. Surveillance is a group of activities conducted by a certifier to ensure ongoing compliance once initial compliance has been determined. Post-market surveillance involves the evaluation of certified products taken from the marketplace to determine if product requirements continue to be met. Pre-market surveillance is the checking of products before they reach the market and may include audits of the supplier's process control systems and/or inspection of the production. In other certification systems, surveillance is accomplished by requiring all or some significant part of the activities used initially to determine compliance to be re-conducted on a periodic basis. This recertification process can take the form of retesting or re-assessing the characteristics of interest at prescribed intervals. Certification is very useful in situations that involve mass-produced products and characteristics that cannot be readily inspected.

[28] See http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-204.

Many private organizations, as well as federal and state agencies in the United States, certify products ranging from electrical cords to meat products. In addition, many certification programs are operated at local government (city, township, county, etc.) levels. Consumers see evidence of the extensiveness of certification-related activities when they see, for example, the Underwriters Laboratories (UL) mark on such diverse products as electric coffee pots and fire extinguishers or when they see the NSF mark on products ranging from plumbing equipment to food and beverage vending machines. The U.S. Department of Agriculture's (USDA) certification mark can be found on poultry and other agricultural products, while the U.S. Department of Energy's (DOE) Energy Star mark can be found on many electrical and electronic products that have achieved a certain level of energy efficiency. These are only a few of the many certification marks which may appear on consumer products.

Conformity Assessment Functional Overview

Figure B1 provides a functional overview of CA and the relationship among certification bodies, testing laboratories, laboratory accreditation bodies, product developers, and owners of Qualified Products Lists (QPL). The success of the accreditation and conformity process requires that the procurement agencies, laboratories, and laboratory accreditation authorities have a clear understanding of the requirements and test tools mandated by the accreditation authority. The laboratory accreditation process provides formal recognition that a laboratory is competent to carry out specific tests or calibrations or types of tests or calibrations.

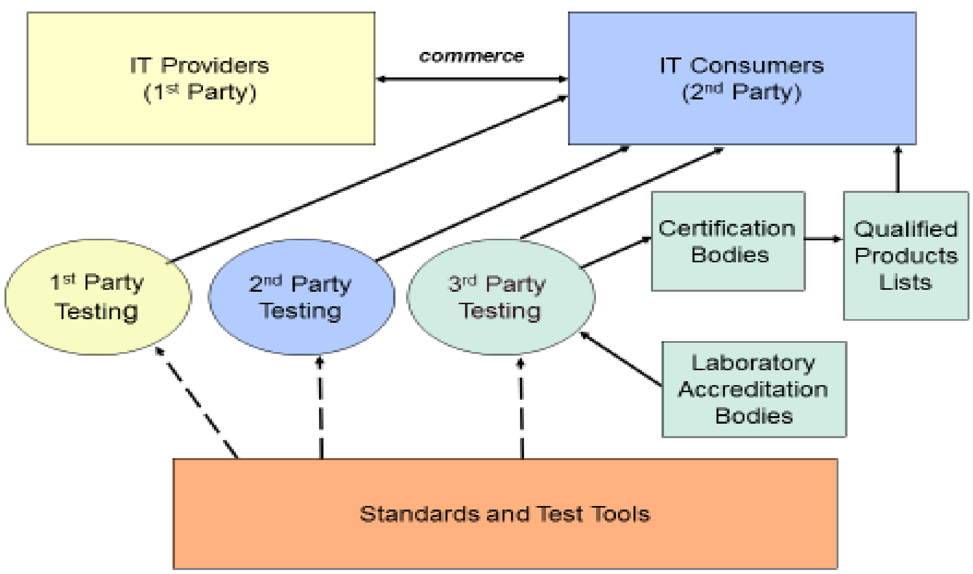


Figure B1 Conformity Assessment Functional Overview

Annex C – USG Legislative and Policy Mandates for Cybersecurity

Biometrics

- USA PATRIOT Act (Public Law 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (Public Law 107-173)
- Homeland Security Presidential Directive/HSPD #12: Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004)
- National Security Presidential Directive/NSPD #59/ Homeland Security Presidential Directive/HSPD #24, Biometrics for Identification and Screening to Enhance National Security (June 5, 2008)

Cybersecurity

- Cybersecurity Enhancement Act of 2014 (Public Law No: 113-274)
- Improving Critical Infrastructure Cybersecurity (Executive Order, February 12, 2013)
- National Cybersecurity Center of Excellence (Public Law 112-55, Consolidated and Further Continuing Appropriations Act of 2012)
- National Initiative For Cybersecurity Education (NICE)
- Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) [supersedes Computer Security Act of 1987 (Public Law 100-235)]
- Federal Information Security Management Act (FISMA) of 2002 (Title III of the E-Government Act Federal Information Security Management Act of 2002 (Public Law 107-347)
- Cybersecurity Research and Development Act of 2002 (Public Law 107-305)
- National Strategy to Secure Cyberspace (February 2003)
- Homeland Security Presidential Directive #12: Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004)
- Conference Report on House Resolution 5441, Department of Homeland Security Appropriations Act, 2007: Title V - General Provisions (WHTI [Western Hemisphere Travel Initiative] Certification effort)
- OMB Circular A-130 Management of Federal Information Resources (February 8, 1996)
- OMB M-04-04 E-Authentication Guidance for Federal Agencies (December 16, 2003)
- OMB Directive 05-24 Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (August 5, 2005)
- OMB Memorandum M-08-05, Implementation of Trusted Internet Connections (November 20, 2007)
- OMB M-08-23 Securing the Federal Government's Domain Name System Infrastructure (August 22, 2008)
- National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23): Comprehensive National Cybersecurity Initiative (January 2008)

Emergency Alert for Wireless Mobile Devices

- Warning, Alert, and Response Network Act (part of the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) (Public Law 109-347)

Healthcare Information Technology

- Health Information Technology for Economic and Clinical Health (HITECH) Act, American Recovery and Reinvestment Act of 2009 (Public Law 111-5)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191)

Identity Management

- National Strategy for Trusted Identities in Cyberspace (April 2011)

Internet Protocol version 6 (IPv6)

- OMB Memo on Transition to IPv6 (September 28, 2010)
- OMB M-05-22 on Transition Planning for IPv6 (August 2, 2005)

SmartGrid

- Energy Independence and Security Act (EISA) of 2007 (Public Law 110-140)
- American Recovery and Reinvestment Act of 2009 (Public Law 111-5)

Voluntary Voting System Standards

- Military and Overseas Voter Empowerment (MOVE) Act of 2009
- Help America Vote Act of 2002 (Public Law 107-252)

Annex D – Cybersecurity Analysis of Application Areas

This Annex provides a cybersecurity analysis for each of the IT application areas highlighted in Section 4 and Table 1.

D.1 Cloud Computing[29]

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five main characteristics, three service models, and four deployment models.

Essential Characteristics:

- *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants (PDAs)).
- *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- *Rapid elasticity.* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and be rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- *Measured Service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at a level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

- *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual

[29]NIST Special Publication 800-145, NIST Definition of Cloud Computing, September 2011.

application capabilities, with the possible exception of limited user-specific application configuration settings.

- *Cloud Platform as a Service (PaaS)*. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

- *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premise.
- *Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Threats

The “Cloud First” policy makes cloud computing the new norm for government agencies. However, if not properly addressed, federal information and information systems[30] are subject to serious threats that can have adverse impacts on organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation[31] by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. The adoption of cloud computing marks the beginning of a new technological era that calls for additional guidance for agencies of how to best assess and manage the risk assumed from adopting this new technology that changes the

[30] A *federal information system* is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
[31] Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

emphasis of the traditional IT services from procuring, maintaining, and operating the necessary hardware and related infrastructure to the business' mission, and delivering value added capabilities and services at lower cost to users.

The three cybersecurity objectives, ensuring the confidentiality, integrity, and availability of information and information systems, are particularly relevant, in addition to privacy, as these are the high priority concerns and perceived risks related to cloud computing. Consistent with other Application Areas, cloud computing implementations are subject to local physical threats, including insider threats, as well as remote, external threats. For majority of Application Areas, the source of these threats includes accidents, natural disasters, hostile governments, criminal organizations, terrorist groups, malicious or unintentional introduction of vulnerabilities through internal and external authorized and unauthorized human and system access, including but not limited to employees and intruders. While the security of a cloud computing ecosystems may be affected by similar threat vectors, the cloud's architectural native characteristics such as *rapid-elasticity* and *broad network access*, increase the cloud service's availability and potentially can, on the positive side, prevent the loss of service during natural disasters. On the negative side, the multi-tenant model used to support the *resource pooling* characteristic requires careful architectural considerations and mechanisms in place to provide logical, vertical isolation of data, in such a way that no tenant can intentionally or unintentionally get access to another tenant's data.

Overall, cloud computing's three service types and four deployment models heighten the need to develop data-centric architectures that consider data and systems protection in the context of logical as well as physical boundaries. Additionally, forensics investigations are more challenging in cloud ecosystems than traditional IT systems due to cloud native characteristics and architecture.

Possible types of attacks against Cloud Computing services include the following:

- Compromises to the confidentiality and integrity of data in transit to and from a cloud provider;
- Compromises to the confidentiality and integrity of data at rest (when not in use);
- Compromises to the confidentiality and integrity of data in memory (when data is in use)
- Attacks which take advantage of the homogeneity and power of cloud computing environments to rapidly scale and increase the magnitude of the attack;
- Unauthorized access (through improper authentication or authorization, or vulnerabilities introduced during maintenance) to software, data, and resources in use by a cloud service consumer by another consumer;
- Inadequate cryptographic key management when encryption is extensively used to prevent data disclosure in multi-tenant environments;
- Increased levels of network-based attacks that exploit software or vulnerabilities in applications designed for private networks and not using an Internet threat model;
- Portability and interoperability constraints resulting from non-standard application programming interfaces (APIs) and lack of data format standardization cause vendor lock-in and cloud consumer's inability to change cloud service provider and promote competitiveness;

- Attacks that take advantage of virtual machines that have not recently been patched because they have not been in use; and
- Attacks that exploit inconsistencies in global privacy policies and regulations.

Security Objectives

Major security objectives for cloud computing ecosystems include the following:

- **Define cloud-adapted information security management system (a cloud-adapted risk management framework, with a cloud consumer centric approach**.) This includes the *trust boundary* concept – a logical boundary that identifies, from the consumer's perspective, all the security controls the system inherits or uses directly, including the ones implemented by other actors, and it is essential for the risk management process and security authorization of the acquired cloud service.

- **Define a methodology that allows for clear identification and delineation of security and privacy responsibilities between service provider(s), broker(s) and consumer.** This is important since it provides the foundation for the SLA negotiation (including security SLA) and the security metrics used to monitor the acquired cloud service.

- **Protect consumer's data from unauthorized disclosure or modification.** Even though access control to data is a key part of the risk management, re-iterating its importance by identifying it as a separate objective is essential. This includes supporting identity management such that the customer has the capability to enforce identity and access control policies on users accessing cloud services. The objective can include consumer's ability to grant access to its data selectively, available to other authorized entities (data sharing management capability).

- **Providing guidance for Security SLA & metrics.** This is directly correlated with the overall Service Level Agreement (SLA). The objective is also setting the foundation for the continuous diagnostic and mitigation and continuous monitoring of cloud service.

- **Support portability such that the customer can take action to change cloud service providers when needed to satisfy availability, confidentiality and integrity requirements.** This includes the ability to close an account on a particular date and time, and to copy data from one service provider to another.

- **Proper cryptographic key management solutions for keys used for data confidentiality and integrity protection and for keys used for users' identification (when applicable).** This objectives ensures that data encryption, data signing and users' identification mechanisms do not give a false sense of security and keys do not become accessible to unauthorized entities**;**

- **Prevent unauthorized access to cloud computing infrastructure resources.** This includes implementing security domains that have logical separation between computing resources (e.g. logical separation of customer workloads running on the same physical server by virtual machine [VM] monitors [hypervisors] in a multitenant environment) and using secure-by-default configurations.

- **Design web applications deployed in a cloud using an Internet threat model.** This objective promotes best practices for web applications in general, including the cloud-based ones, by highlighting the need to embed security into the software development process.

- **Protect Internet browsers from attacks to mitigate end-user security vulnerabilities.** This includes taking measures to protect internet-connected personal computing devices by applying security software, personal firewalls, and patch maintenance.

- **Monitor access control and intrusion detection mechanisms implemented by cloud provider and broker, and design independent assessment mechanism to verify they are in place.** This includes (but does not rely on) traditional perimeter security measures in combination with the domain security model. Traditional perimeter security includes restricting physical access to network and devices, protecting individual components from exploitation through security patch deployment, default most secure configurations, disabling all unused ports and services, role based access control, monitoring audit trails, minimizing the use of privilege, antivirus software; and encrypting communications.

Standards Landscape

NIST Special Publication 500-291 version 2, NIST Cloud Computing Standards Roadmap, July 2013, surveyed the existing standards landscape for interoperability, performance, portability, security, and accessibility standards relevant to cloud computing. Using this available information, current standards, standards gaps, and standardization priorities are identified within this document.

The communication between end-users and cloud ecosystem is supported by existing standards that have been developed to facilitate communication, data exchange, and security, such as base-level infrastructure standards, (e.g. TCP/IP, DNS, SMTP, HTML, HTTP, HTTPS, FTP,) These standards offer a convenient and secure access to cloud-based information systems, while restricting majority security exposures of data in transit. Other standards such as SSL and TLS provide public-key cryptographic protocols that allow customers and cloud providers to automatically establish shared keys that can be used to protect their communications (although much yet remains to be done in this space).

Other security standards that are relevant to cloud computing include XACML (eXtensible Access Control Markup Language) and SAML (Security Assertion Markup Language). A number of additional web-oriented standards exist, including the WS (Web Services) standards such as WS-Trust, WS-Policy, WS-SecurityPolicy, etc., but their adoption by the market place is limited.

Cloud security related standards development in JTC 1 SC 27, IT Security Techniques, has resulted in some approved standards with more under development. ISO/IEC 27040:2015 provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. Draft standard ISO/IEC DIS 27017 will provide guidance on the information security elements of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002. Draft standard ISO/IEC CD 27036-4 will provide guidance for security of cloud services in supplier relationships. JTC 1 SC 27 is also investigating the need for standards for a Cloud Adapted Risk Management Framework and for Virtualization Security.

D.2 Emergency Management

The first responder community needs reliable, secure, and interoperable information and communications technology to protect the public during disasters and catastrophes. There is increasing convergence of the voice, data, and video information being exchanged to provide situational awareness in response to an event. For larger disasters and catastrophes, first responders from neighboring jurisdictions or inter-governmental jurisdictions (i.e., state or Federal) need to be integrated into the response, along with the information and communications technologies they use.

Threats

Historically, the first responder community has not operated their communication and data systems as a single entity, rather by jurisdiction, region, or by Federal agency. The increased use of broadband-based applications and infrastructure by emergency response agencies stands to make emergency communications systems more vulnerable to cyber-attacks. As a result, agencies should address cybersecurity in their planning efforts and coordinate with their partners to ensure shared resources are secured from cyber-attacks. Currently, there is an effort to build a nationwide public safety broadband network in the 700 MHz spectrum that would initially provide data access and eventually voice services. As this nationwide network is built out, a need for cybersecurity awareness will increase. Threats include possible blended attacks and disasters: a physical catastrophe combined with the disruption of the information and communications technology, affecting one or more characteristics (availability, confidentiality, and/or integrity). Supply chain threats to the integrity and reliability of network components must also be considered. As a national network is rolled out and emergency response agencies move towards broadband-enabled networks and devices, their communications will likely be transmitted over commercial infrastructures, making them more vulnerable to cyber-attack.

Agencies therefore must make cybersecurity a priority and begin building expertise in cybersecurity preparedness to ensure that their networks can prevent, deter, and mitigate cyber-attacks while reducing their physical and logical vulnerabilities. In the near term, agencies need to implement features for end-to-end cybersecurity, such as authentication and encryption, and coordinate with their partners to ensure shared resources are secured from physically and cyber-attacks.

Security Objectives

As the nationwide network is built out and the users of the systems incorporate its use in day-to-day operations, cybersecurity issues should be addressed in each agency's standard operating procedures. Also, as the network is built out, cybersecurity features should address network vulnerabilities, which typically occur due to a deficiency in cybersecurity standardization across communication and information systems.

Some core areas of cybersecurity standardization that need to be addressed for first responders include the following:

- Identity management – Each first responder or public safety user needs to be authenticated onto their home network or a visitor network if they are roaming.
- Information security management systems – First responders' connections to records management systems and related databases need to be protected.
- Network security – Overall cybersecurity throughout the nationwide network, including encryption (for confidentiality and integrity), based on long term evolution (LTE) technology is required.
- Supply chain security – The integrity and reliability of suppliers and the components they provide, or serve as integrators of, for first responders or public safety users need to be considered.

Standards Landscape

The emergency management and business continuity community comprises many different entities, including the government at distinct levels (e.g., Federal, State, local governments); business and industry; nongovernmental organizations; and individual citizens. Each of these entities has its own focus, unique missions and responsibilities, varied resources and capabilities, and operating principles and procedures.

Interoperability in public safety networks has been identified as a pressing issue in both the 9-11 Commission Report and the Federal assessment of the response to Hurricane Katrina. Both events revealed the inability of public safety personnel to communicate with people from other agencies due to conflicting standards and the lack of adequate communications infrastructure. This led to an inefficient response to rapidly changing circumstances and, especially in Manhattan, a high casualty rate among front-line public safety personnel. As new wireless networks are developed by SDOs such as 3GPP and IEEE 802, determining if these emerging standards-based technologies are suitable for meeting public safety needs is an ongoing issue.

To minimize the impact of disasters, terrorist attacks and other major incidents, ISO has developed a standard for emergency management and incident response: ISO 22320:2011, Societal security – Emergency management – Requirements for incident response. ISO 22320 outlines global best practice for establishing command and control organizational structures and procedures, decision support, traceability and information management.

At the U.S. level, the Emergency Management Accreditation Program (EMAP) has developed and maintains on a three-year cycle a set of 64 standards (The Emergency Management Standard) by which State and local government programs that apply for EMAP accreditation are evaluated.

The National Fire Protection Program (NFPA) has developed and maintains NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs. This standard establishes a common set of criteria for all hazards disaster/emergency management and business continuity programs. NFPA 1600 has been adopted by the U.S. Department of Homeland Security as a voluntary consensus standard for emergency preparedness.

NFPA also develops and maintains standards for devices used by first responders. The 2013 NFPA 1981: Standard on Open-Circuit Self-Contained Breathing Apparatus (SCBA) for Emergency Services, establishes levels of respiratory protection and functional requirements for SCBA used by emergency services personnel. The 2013 NFPA 1982: Standard on Personal Alert Safety Systems (PASS), covers labeling, design, performance, testing, and certification for PASS that monitor an emergency responder's motion and automatically emit an audible alarm if the responder becomes incapacitated -- allowing the PASS to be manually activated if assistance is needed.

D.3 Industrial Control Systems (ICS)

Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations. ICS are critical to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems.

Many of today's ICS evolved from the insertion of IT capabilities into existing physical systems, often replacing or supplementing physical control mechanisms. For example, embedded digital controls replaced analog mechanical controls in rotating machines and engines. Improvements in cost-performance have encouraged this evolution; resulting in many of today's "smart" technologies such as smart transportation, smart buildings, and smart manufacturing. While this increases the connectivity and criticality of these systems, it also creates a greater need for their adaptability, resiliency, safety, and security. The introduction of IT capabilities to promote corporate connectivity and remote access into physical systems presents emergent behavior that has security implications.

ICS now use many standard IT protocols, such as TCP/IP networking, HTTP, File Transfer Protocol (FTP), and Extensible Markup Language (XML).

Threats

Originally, ICS implementations were susceptible primarily to local threats because many of their components were in physically secured areas and the components were not connected to IT networks or systems. However, the trend toward integrating ICS systems with IT solutions provides significantly less isolation for ICSs from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats. Also, the increasing use of wireless networking places ICS implementations at greater risk from attackers who are in relatively close physical proximity but do not have direct physical access to the equipment. Accordingly, threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters. Malicious or accidental actions by insiders can result in damage, as well. Protecting the integrity and availability of ICS systems and data is typically of utmost importance, but confidentiality is another important concern.

Possible types of attacks against ICS systems include the following:

- Delaying or blocking the flow of information through ICS networks, which could disrupt ICS operation;
- Making unauthorized changes to instructions, issuing unauthorized commands, and changing alarm thresholds, which could potentially damage, disable, or shut down equipment;
- Sending false information to system operators either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions;
- Modifying the ICS software or configuration settings, or infecting the ICS with malware, which could have various negative effects; and

- Interfering with the operation of safety systems, which could endanger human life and result in environmental hazards.

Although many IT security controls could be used as a starting point for ICS systems, special considerations must be taken when introducing these controls to ICS environments. ICSs have many characteristics that differ from traditional Internet-based information processing systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation's economy, and compromise of proprietary information. ICSs have different performance and reliability requirements and often use operating systems and applications that are not supported properly by IT security controls. Furthermore, the goals of safety and security must be reconciled with the design and operation of ICSs.

Security Objectives

Major security objectives for an ICS implementation often include the following:

- **Restrict logical access to the ICS network and network activity.** This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the enterprise and ICS networks, and having separate authentication mechanisms and credentials for users of the enterprise and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restrict physical access to the ICS network and devices.** This includes using a combination of physical access controls, such as locks, card readers, and/or guards, to prevent unauthorized physical access to components which could cause serious disruption of the ICS's functionality.
- **Protect individual ICS components from exploitation.** This includes deploying security patches rapidly, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to detect, prevent, deter, and mitigate malware.
- **Maintain functionality during adverse conditions.** This involves designing the ICS so that each critical component has a redundant counterpart, so that when failures occur the components fail gracefully to prevent catastrophic cascading events.
- **Build a culture of reliability, security and resilience for controls systems, components and supporting architecture.** This includes promoting the acceptance of and adherence to a set of codified ICS cybersecurity standards appropriate for each sector.
- **Coordinate ICS cybersecurity efforts among federal, state, local, and tribal governments, as well as owners, operators and vendors.** This involves reducing the likelihood of success and severity of impact of a cyber-attack against critical infrastructure control systems through risk mitigation activities.

Standards Landscape

ICS cybersecurity standards are being developed by several SDOs, including ISA, IEC, and IEEE.

The Industrial Society of Automation (ISA), through the ISA99 committee, is developing and establishing standards, technical reports and related information that will define procedures for implementing electronically secure industrial automation and control systems, security practices, and assessing electronic security performance. This suite of standards, ISA/IEC 62443: Security for Industrial Automation and Control Systems is the result of a strong collaborative relationship between ISA99 and IEC TC65 WG10.

Examples of broadly applicable cybersecurity standards for ICS are the IEEE 802 local area network standards.

Gaps in current ICS cybersecurity standards development include finalized metrics standards and business case development to incentivize application of ICS cybersecurity standards with limited resources of ICS owners and users.

D.4 Health Information Technology

The adoption and use of health information technology promises an array of potential benefits for individuals and the U.S. healthcare system through improved clinical care and reduced cost. At the same time, this environment also poses new challenges and opportunities for safeguarding individually identifiable health information, and maintaining trust in technology implementations intended to facilitate the use and exchange of electronic health information. The overarching privacy and security goal of this application area is to build public trust and participation in HIT and electronic health information exchange by incorporating effective privacy and security solutions in every phase of its development, adoption, and use.

Threats

Ensuring the confidentiality, integrity, and availability of health information is critical to providing high quality, coordinated patient care and maintaining trust in HIT. Much like other application areas, threat sources may include accidents, natural disasters, external loss of service, criminal activity, equipment failures, user errors, and intentional and unintentional exposures of personal health information by authorized or unauthorized personnel.

Security Objectives

In general, the meaningful use of HIT will help to ensure adequate privacy and security protections for personal health information. The security objectives of HIT revolve around the implementation of security controls that provide for the confidentiality, integrity, and availability of patient information and for the systems supporting the use and exchange of that information.

Major security objectives for this application area include the following:

- Protect patient information from unauthorized disclosure or modification;
- Ensure patient information is available to authorized entities when it is needed;
- Explore and promote, where appropriate, existing and emerging technologies to enhance security and privacy of health information; and
- Educate HIT consumers on security and privacy issues related to the uses of HIT and protected health information.

Standards Landscape

Many existing national and international cybersecurity standards, specifications, and technical frameworks can be applied to the HIT application area to provide core cybersecurity capabilities. Communication security is supported by many existing standards such as base-level infrastructure standards, (e.g. TCP/IP, DNS, SMTP, HTML, HTTP, HTTPS, FTP,) These standards can offer a convenient and secure access to HIT information systems, while restricting majority security exposures of data in transit. Other standards such as SSL and TLS provide public-key cryptographic protocols that allow customers and cloud providers to automatically establish shared keys that can be used to protect their communications.

However, with the increasing focus on HIT, there is a need for more mature standards that are directly applicable to, and developed within the context of, this application area.

D.5 Smart Grid

The electric power industry is ready to make the transformation from a centralized, producer-controlled network to one that is less centralized and consumer-interactive. The move to a smarter electric grid promises to change the electric industry much like the Internet has changed the way we communicate. Twenty years ago, few people were utilizing the Internet. Today the Internet has revolutionized many aspects of our lives. The Smart Grid represents an extension of this movement towards a change in power usage. Deployment of various Smart Grid elements, including smart sensors on distribution lines, smart meters in homes, and widely dispersed sources of renewable energy, is already underway and will be accelerated as a result of federal Smart Grid Investment Grants and other incentives.

Threats

The implementation of the Smart Grid will rely on the IT infrastructures in ensuring the reliability and security of the electric sector. Therefore, the security of systems and information in the IT and telecommunications infrastructures must be addressed by an evolving electric sector. Security must be included in all phases of the system development life cycle, from design phase through implementation, maintenance, and disposition/sunset.

Cybersecurity must address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. The need to address potential vulnerabilities has been acknowledged across the federal government.

Additional risks to the grid include:

- Increased complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors;
- Interconnected networks can introduce common vulnerabilities resulting in a domino effect – a cascading series of failures across the grid;
- Increasing vulnerabilities to communication disruptions and the introduction of malicious software/firmware or compromised hardware could result in denial of service (DoS) or other malicious attacks;
- Increased number of entry points and paths are available for potential adversaries to exploit;
- Interconnected systems can increase the amount of private information exposed and increase the risk when data is aggregated;
- Increased use of new technologies can introduce new vulnerabilities; and
- Expansion of the amount of data that will be collected that can lead to the potential for compromise of data confidentiality, including the breach of customer privacy.

Security Objectives

In its broadest sense, cybersecurity for the electric power industry covers all issues involving automation and communications that affect the operation of electric power systems and the functioning of the utilities that manage them and the business processes that support the customer base. In the power industry, the focus has been on implementing equipment that can improve power system reliability. Until recently, communications and IT equipment were typically seen as supporting power system reliability. However, increasingly these sectors are becoming more critical to the reliability of the power system. For example, in the August 14, 2003, blackout, a contributing factor was issues with communications latency in control systems. With the exception of the initial power equipment problems, the ongoing and cascading failures were primarily due to problems in providing the right information to the right individuals within the right time period. Also, the IT infrastructure failures were not due to any terrorist or Internet hacker attack; the failures were caused by inadvertent events—mistakes, lack of key alarms, and poor design. Therefore, inadvertent compromises must also be addressed, and the focus must be an all-hazards approach.

Standards Landscape

Traditionally, cybersecurity for IT focuses on the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Cybersecurity for the smart grid requires an expansion of this focus to address the combined IT, ICS, and communication systems, and their integration with physical equipment and resources in order to maintain the reliability and the security of the smart grid and to protect the privacy of consumers. Smart grid cybersecurity must include a balance of both electricity- and cyber-system technologies and processes in IT and in ICS operations and governance.[32]

NIST Special Publication 1108r3, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, includes a review of cybersecurity standards relevant for the Smart Grid. Table 4-1 now identifies 71 smart grid-relevant standards. Sixteen standards or relevant publications, which specifically address cybersecurity, are listed together as a group in the table.

[32] NIST Special Publication 1108r3, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0

D.6 Voting

The most familiar part of a voting system is the mechanism used to capture the citizenry's choices or votes on ballots. In addition to the vote capture mechanism, a voting system includes voter registration databases and election management systems. Voter registration databases contain the list of citizens eligible to participate in a jurisdiction's election. Voter registration databases populate poll books used at polling places to verify one's eligibility to participate in an election and ensure they received the correct ballot style. The election management system is used to manage the definition of different ballot styles, configuration of the vote capture mechanism, collection and tallying of cast ballots, and creation of election reports and results. The information flowing throughout the voting systems can be in paper or electronic form.

The voting system in the United States is decentralized so the various States can choose the type of voting systems they wish to use to support and conduct their elections. Examples of some types of voting systems used in the United States are:

- Optical Scan systems where voters marks their choices (such as filling in an oval with a pen or pencil) on paper ballot; and election reports are created by running the marked ballots through a scanner so choices can be tallied.
- Directed Recording Electronic (DRE) voting systems where voters make their choices using a touch screen; and election reports are created by collecting and processing the electronically recorded cast ballots.
- DRE with Voter Verifiable Paper Audit Trail (VVPAT) are the same DREs but an additional paper record is created with the voter's choices that a voter can verify if they want and can be used to audit the accuracy of electronically generated reports and tallies.

As a result of the issues with punch card voting systems used in the 2000 election, the Help America Vote Act (HAVA) of 2002, enacted to improve and update the voting systems used throughout the United States, established the Election Assistance Commission (EAC). One of the EAC's responsibilities is to create voluntary voting systems guidelines and establish a national voluntary testing and certification program for voting systems used in State and Federal elections. Until recently, the focus of the voting system guidelines have been for polling place voting systems where one goes to a specific polling place to cast their ballot. With the enactment of the Military and Overseas Voter Empowerment (MOVE) Act of 2009, States are required to provide election material via electronic communications to military and overseas absentee voters. In addition, the MOVE act calls for the development of standards for electronic absentee voting systems.

Threats

Past work on voting systems have focused on paper-based polling place voting systems, where a variety of local threats to voting system equipment and election data exist. Earlier work on standards and guidelines for polling place voting systems focused on ensuring the reliability of voting system equipment in the face of hardware failures and environmental threats, and minimizing the risks of accidental or malicious misuse of voting system equipment or data by voters and polling place staff with physical access.

The move to electronic voting systems has resulted in a new threat environment, while simultaneously creating opportunities for implementing additional technical security controls to combat these new threats. In addition to malicious or accidental misuse of electronic voting systems by those with physical access to electronic voting machines before, during or after elections, individuals charged with designing, implementing, configuring or deploying electronic voting systems may be in a position to tamper with equipment. The electronic voting systems must also be protected in-storage between elections, as equipment could be tampered with long before any elections take place.

Current work on voting system standards and guidelines is directed at remote electronic voting for overseas and military voters, further changing the threat environment to include Internet-based threats, and hostile individuals or groups capable of inflicting damage from remote locations.

In general, possible attacks against voting systems may be directed at:

- **Changing the results of the election.** Accidental or malicious attacks could result in the modification of votes after being cast, or could cause systems to malfunction and incorrectly store or tabulate cast ballots.
- **Violating ballot secrecy or voter privacy.** Improperly designed, implemented or deployed voting systems could allow individuals to observe how a voter voted. Individuals or groups, particularly those with logical or physical access to voting systems, could gain unauthorized access to how individuals voted in the election.
- **Disruption of voting.** Hardware and software failures, and potential malicious attacks including denial of service attacks, may disrupt the voting process, or even result in the loss of cast ballots.
- **Creating distrust in the election outcome.** Some small-scale attacks may not be capable of changing the results of an election, but could have a negative effect on the public’s trust in elections.

Security Objectives

Voting systems have a unique set of security objectives. Election results must be auditable while also protecting the secrecy of cast ballots, even from those auditing the election systems and results. Proper security controls must be implemented on systems, while also keeping the voting systems easy to use by the aging poll worker population and voters. Systems must carefully balance the needs of each of these objectives.

Major security objectives for voting systems include the following:

- **Accuracy:** Voting systems should accurately capture, store and tabulate cast ballots.
- **Integrity**: Voting system integrity typically includes protection of voting system software as well as important election records, including voter registration databases, blank ballots and candidate lists, cast ballots, and tabulation reports.
- **Auditability:** It should be possible to independently verify the results of the election.

- **Voter Privacy:** The voting system should protect the secrecy of the selections that voters make from unauthorized observation at the polling place.
- **Reliability:** Voting systems should be designed so that they will function properly during an election. In the event of a failure, the system should be designed to prevent catastrophic failures that could lead to the loss of cast ballots.
- **Transparency:** Public observers should be able to monitor the elections process and verify that equipment is functioning correctly and that proper procedures are adhered to.
- **Usability and Accessibility:** Voting systems should be designed so that election staff can easily operate equipment without errors, and so that all voters are able to cast valid votes as intended, without errors, and with confidence that their ballots choices were recorded correctly.

Standards Landscape

In the United States, standards for electronic and paper based polling place voting systems are promulgated by the EAC as the Voluntary Voting System Guidelines (VVSG). The EAC administers an accreditation program for testing laboratories that tests the conformance of voting system equipment to the requirements found in the VVSG. As a result of the MOVE Act, interest in guidelines for remote electronic voting systems has increased, leading the EAC to establish a pilot testing and certification program that currently focuses on remote electronic voting systems from supervised and controlled platforms.

The Institute of Electrical and Electronics Engineers (IEEE) has established the Voting System Electronic Data Interchange project P1622 that is investigating formats to allow voting systems to exchange information electronically. The Organization for the Advancement of Structured Information Standards (OASIS) has established a technical committee on Election and Voter Services that has produced the Election Markup Language (EML) based on the Extensible Markup Language (XML) with the goal of allowing hardware, software, and service providers of election system and service providers to exchange information.

Annex E – Cybersecurity SDO Inventory Matrix

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
3GPP Overall Scope: 3rd Generation Mobile System based on the evolved GSM core networks	n/a	Device integrity & user authentication; location verification; media security	Membership in an organizational partner is a pre-requisite	Public sector Private sector	Consensus by voting	IPR policies from organizational partner respected. Generally grant licenses on fair reasonable terms and conditions and on non-discriminatory basis	Establish a work item then by member contributions Produces technical specifications or technical reports Specifications grouped in releases	DHS/CS&C (I)	IT Industry

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
3GPP2 Overall Scope: 3rd Generation Mobile System based on CDMA (Code Division Multiple Access) technology	n/a	Access Control (bilateral) Authentication of subscriber and network Confidentiality & integrity Key management Data and identity privacy	Membership in an organizational partner is a pre-requisite	Public sector Private sector	Consensus by voting	IPR policies from organizational partner respected. Generally grant licenses on fair reasonable terms and conditions and on a non-discriminatory basis	Submission of work proposal Produces technical specifications or technical reports	DHS/CS&C (I)	IT Industry

Standards Developer	**U.S. Member**	**Cyber Security Scope**	**Membership**	**Standards User Community**	**Decision Making**	**IPR Policy**	**Process**	**USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities**	**Private Sector Participation**
ATIS Overall Scope: Existing and next generation IP-based infrastructures	n/a	Network Reliability Mobile System Security	Organization	Public sector Private sector	Consensus by voting	Copy-righted standards For sale RAND or RF For essential patents and essential claims			IT Industry

Standards Developer	**U.S. Member**	**Cyber Security Scope**	**Membership**	**Standards User Community**	**Decision Making**	**IPR Policy**	**Process**	**USG Agency Participation** **See section 15 for explanation of these terms:** **M=monitor** **I=influence** **L=lead** **P= in limited specific activities**	**Private Sector Participation**
IEC TC 57 Overall Scope: Power systems management and associated information exchange	USNC	Data and Communications Security for Power Systems	National Bodies National Body delegations include individuals from: Industry Government Academia	Public sector Private sector	Consensus by voting	Copy-righted standards For sale RAND or RF for essential patents and essential claims	5-stage process: New Work Item Proposal (NP); Working Draft (WD); Committee Draft (CD); Draft International Standard (DIS); Final Draft International Standard (FDIS); International Standard (IS) Fast track processes		Electrical and Electronic Industry

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
IEC TC 65 Overall Scope: Industrial process measure-ment, control and automation	USNC	Security aspects of Industrial Process Systems	National Bodies National Body delegations include individuals from: Industry Government Academia	Public sector Private sector	Consensus by voting	Copy-righted standards For sale RAND or RF for essential patents and essential claims	5-stage process: New Work Item Proposal (NP); Working Draft (WD); Committee Draft (CD); Draft International Standard (DIS); Final Draft International Standard (FDIS); International Standard (IS) Fast track processes		Industrial Control Systems Industry

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
IEEE Standards Association Overall Scope: Power; Energy; Healthcare; IT; etc.	n/a	IEEE 802 Local Area Network (LAN)/ Metropolitan Area Networks (MAN) Software and Systems Engineering Group (S2ESC)	Individual or Organization	Public sector Private sector	Consensus by voting	Copy-righted standards For sale and IEEE 802 standards free after 6-month publication date[33] RAND or RF For essential patents and essential claims	Initiate project Develop draft Ballot for approval Recirculate to increase consensus Approval that process was followed	DOC/NIST (L), DOC/NTIA DOJ/FBI, DHS/CS&C (I), FCC	IT Industry Academia

[33] More info can be found at the following link: http://standards.ieee.org/about/get/index.html .

Standards Developer	**U.S. Member**	**Cyber Security Scope**	**Membership**	**Standards User Community**	**Decision Making**	**IPR Policy**	**Process**	**USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities**	**Private Sector Participation**
IETF Overall Scope: Internet	n/a	Internet Security Protocols	Individual	Public sector Private sector	Rough consensus and Running code	Copy-righted standards Freely available Patent disclosure required at time of contribution; favors RANDZ or IPR-free solutions	3 stage process: working group (WG); community; IESG evaluation; RFC 3 levels of maturity for standards track RFCs: Draft; Proposed; Full 2 independent interoperable implementations of every feature required for Draft Standard	DOC/NIST (L), DoD/CIO (I) DoD/NSA, DOJ/FBI, DHS/CS&C (I)	IT Industry Academia

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
ISA Overall Scope: Industrial Control Systems (ICS)	n/a	Cyber security of industrial control systems						DOC/NIST DHS/CS&C (I)	Industrial Control Systems Industry

Standards Developer	**U.S. Member**	**Cyber Security Scope**	**Membership**	**Standards User Community**	**Decision Making**	**IPR Policy**	**Process**	**USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities**	**Private Sector Participation**
ISO/IEC JTC 1 Overall Scope: IT	ANSI is the US member INCITS is ANSI designated US TAG (Technical Advisory Group)	LAN Security; Identification cards & related devices; ID Management; Encryption; ISMS; Common Criteria (CC); Network Security; Biometrics; Software and Systems Engineer-ing; Distribu-ted applica-tion platforms & services	National Bodies National Body delegations include individuals from: Industry Government Academia	Public sector Private sector	Consensus by voting	Copy-righted standards For sale RAND or RF for essential patents and essential claims	5-stage process: New Work Item Proposal (NP); Working Draft (WD); Committee Draft (CD); Draft International Standard (DIS); Final Draft International Standard (FDIS); International Standard (IS) Fast track processes	DHS/CS&C (I), DoD/DISA, DOJ/FBI , DOC/NIST (L), DOC/ITA (P), DoD/NSA, State	IT Industry Academia

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
ISO TC 68 Overall Scope: Banking & Other Financial Services	ANSI is the US member X9, Inc. is ANSI designated US TAG	Secure Electronic Fund Transfers; Encryption	National Bodies National Body delegations include individuals from: Industry Government Academia	Financial services sector	Consensus by voting	Copy-righted standards For sale RAND or RF for essential patents and essential claims	5-stage process: NP;WD;CD; DIS; FDIS; IS Fast track process	DOC/NIST, DoD/NSA	Financial Industry
ITU-R Overall Scope: Radio communication						Copy-righted standards Freely available RAND or RF for essential patents and essential claims			

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
ITU-T Overall Scope: Telecom	Treaty-based organization Department of State is the US member	Telecom Security	National Bodies National Body delegations include individuals from: Industry Government Academia	Telecom sector	Consensus (Voting is an option but rarely exercised)	Copy-righted standards Freely available RAND or RF for essential patents and essential claims	3-stage process: Question; draft Rec; Rec Approval process can be Traditional (TAP) or Accelerated (AAP). Standards may be jointly developed with ISO according to an established process.	State leads delegations that include representatives from any interested USG agency. Depending on the issue, this may include, e.g., DOC/NTIA, FCC, DHS/CS&C (I), DOC/NIST, DoD/NSA, DOJ/FBI, etc.	Telecom Industry, including vendors, operators, consultants. They can participate under company memberships or as part of the U.S. delegation

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
OASIS Overall Scope: Web Services	n/a	Secure Web Services	Individual or Organization	Organizations with web-based services	Consensus by voting	Copy-righted standards Freely available Usually RF for essential patents and essential claims	4-stage process: Committee Draft; Public Review; Committee Specification; OASIS Standard 3 Implementations required before final approval.	DOC/NIST, DHS/CS&C (M)	IT industry

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
PCI SSC Overall Scope: Security Standards for Account Data Protection	n/a	Security Process Standards for Account Data Protection	Organization	Merchants Who Accept Credit Cards, Online or Offline		Copy-righted standards Available with signed license. Covenant not to Assert Patent Claims			Payment Card Industry
TCG Overall Scope: Trusted computing building blocks and software interfaces across multiple platforms	n/a	Trusted computing building blocks and software interfaces across multiple platforms							

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
W3C Overall Scope: Web Technology	n/a	Internet Security	Individual or Organization	Organiza-tions with web-based services	Consensus by voting	Copy-righted standards Freely available RF for essential patents	4-stage process: Working Draft; Candidate Recommendation; Proposed Recommendation; W3C Recommendation Two interoperable implementations are preferred but not required before final W3C approval.	DOC/NIST	IT industry

Standards Developer	U.S. Member	Cyber Security Scope	Membership	Standards User Community	Decision Making	IPR Policy	Process	USG Agency Participation See section 15 for explanation of these terms: M=monitor I=influence L=lead P= in limited specific activities	Private Sector Participation
WiMAX Forum Overall Scope: promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI HiperMAN standard	n/a	Wireless LAN Security; Authentication mechanisms	Organization or individual	Public Sector Private Sector	Consensus	reasonable and nondiscriminatory basis	Working item proposal then contributions	DHS/CS&C (I)	IT Industry