Cyber Security Standards

Karen Scarfone, Dan Benigni and Tim Grance
National Institute of Standards and Technology (NIST), Gaithersburg, Maryland

Abstract: The goal of cyber security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. A cyber security standard defines both functional and assurance requirements within a product, system, process, or technology environment. Well-developed cyber security standards enable consistency among product developers and serve as a reliable metric for purchasing security products.
Cyber security standards cover a broad range of granularity, from the mathematical definition of a cryptographic algorithm to the specification of security features in a web browser, and are typically implementation independent. A standard must address user needs, but must also be practical since cost and technological limitations must be considered in building products to meet the standard. Additionally, a standard's requirements must be verifiable; otherwise, users cannot assess security even when products are tested against the standard.

Keywords: cyber security; information technology; standards; standardization

The International Organization for Standardization (ISO) defines a standard as "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" [1]. Numerous standards have been developed for cyber security to help organizations better manage security risk, implement security controls that meet legal and regulatory requirements, and achieve performance and cost benefits. This article provides an overview of cyber security standards in general and highlights some of the major ongoing international, regional, national, industry, and government standards efforts. It also discusses the advantages of having standards and explains how organizations can participate in standards research and development.

1 Cyber Security Standards Overview

Cyber security standards are proliferating. Governments and businesses increasingly mandate their implementation. More manufacturers and vendors are building and selling standards-compliant products and services. In addition, a growing number of organizations are becoming involved in standards development. Cyber security standards are being embraced because they are useful. They provide tangible benefits that justify the time and financial resources required to produce and apply them.

Security technology has not kept pace with the rapid development of IT, leaving systems, data, and users vulnerable to both conventional and innovative security threats. Politically motivated adversaries, financially motivated criminals, mischievous attackers, and malicious or careless authorized users are among the threats to systems and technology that have the potential to jeopardize cyber security, US economic security, consumer identities and privacy, and US public health and safety. While it is impossible to eliminate all threats, improvements in cyber security can help manage security risks by making it harder for attacks to succeed and by reducing the effect of attacks that do occur.

Cyber security standards enhance security and contribute to risk management in several important ways. Standards help establish common security requirements and the capabilities needed for secure solutions. For example, Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, establishes standard requirements for all cryptographic-based security systems used by federal organizations to protect sensitive or valuable data [2]. Conformance testing can then be performed against the standard to provide assurance to users that cryptographic modules are built to requirements.

Security standards facilitate sharing of knowledge and best practices by helping to ensure common understanding of concepts, terms, and definitions, which prevents errors. For example, the Information and Communications Technology (ICT) Security Standards Roadmap [3] includes references to several security glossaries, including the ISO/IEC JTC1/SC27 IT Security Terminology publication [4]. Other helpful resources include the Internet Security Glossary from the Internet Engineering Task Force (IETF), Request for Comments (RFC) 4949 [5] and a compendium of the International Telecommunications Union Telecommunication Standardization Sector (ITU-T)

approved security definitions [6]. Using common definitions for security terminology saves time in the development of new standards and supports the interoperability of standards.

Cyber security standards also provide other benefits. Because standards generally incorporate best practices and conformance requirements, their use typically results in improvements in quality. Standards reduce the number of technical variations and allow consumers easy access to interchangeable technology. Standards compliance programs offer a way to measure products and services against objective criteria and provide a basis for comparing products, such as confirming that they offer certain sets of security features. Consumers often benefit from cost savings that result from the development, manufacture, sales, and delivery of standards-based, interoperable products and services. Another benefit of cyber security standards is that the standards development process, with its typical practices of involving a wide range of subject-matter experts, prototyping, and incorporating conformity assessment criteria and methodologies, helps ensure that standards are implementable and reflect recommended practices. Products or services that have been demonstrated to conform to IT security standards can then be expected to offer more assurance than nonstandard products.

When security standards are not available for a technology, several problems often occur. Organizations that adopt the technology may not be aware of its inherent security weaknesses and the implications of implementing the technology for the organization's security posture. Organizations also may not have reliable information on how to take advantage of the technology's security capabilities or on what additional security controls may be needed to compensate for weaknesses in those capabilities. This tends to lead to insecure implementations and insufficient security maintenance, making systems more likely to be exploited and the organization more vulnerable to harm.

1.1 Cyber Security Standards Characteristics

Standards can be defined as widely used rules or specifications for activities or their results. Nevertheless, there are often significant differences in how individual standards are developed and applied. These differences can help determine how quickly and easily a new standard is embraced and thereby influence the continued use or demise of alternatives. As a result, standards are often described by the specific characteristics of their development and intended application, including the development process used to produce the standard, the way in which the standard is regulated, the applicability of the standard to different audiences, the availability of the standard to the public, and the measurability of the standard.

Standards come into being in different ways. *Proprietary* or *company standards* are developed by companies with little or no participation by external parties. *De facto standards* are created through the informal adoption of prevailing practices or norms. The majority are *voluntary standards* developed through some form of voluntary consensus process, in which stakeholders participate and agree. Some voluntary standards development efforts are open to all interested parties, while others are restricted to specific groups or individuals, such as members of a particular alliance or consortium.

Standards differ in the ways that they are regulated. Compliance with standards may be optional, or a governing or regulatory organization may make compliance a requirement. *Voluntary standards* are generally called *voluntary*, not only because they are created through volunteers' efforts but also because they are intended for optional use, although a regulating agency could adopt or mandate their use. *Mandatory standards* are standards whose use is prescribed by a regulatory agency or implementing organization. Mandatory standards typically implement laws and regulations.

The audience to whom a standard applies depends upon the entity that develops or adopts it. An *international standard* is one that is adopted by an international standards development organization (SDO) and made available to the public, such as ISO International Standards. A *regional standard* is a standard adopted by several nations in a particular geographic region, for example, European Committee for Standardization (CEN) standards. A *national standard* is a standard developed for use in a particular country either by a government entity or a national SDO. A national standard can also be an international standard that is adopted for use by an individual country. Examples include FIPS and American National Standards Institute (ANSI) standards in the United States and British Standards Institution (BSI) Standards in the United Kingdom. An *industry standard* is one that has been adopted by a particular industry for common use, for example, Security Industry Association (SIA) standards. Finally, a *company standard*, also known as a *proprietary standard*, is a standard developed and owned by a commercial entity that specifies practices or conventions unique to that entity.

Standards may or may not be freely accessible by everyone. By definition, *open standards* are publicly available, but their developer may charge for copies. Examples of open standards that are available to the public for a fee are ISO standards and standards developed by ANSI-accredited organizations. A vendor who develops and owns a *proprietary standard* may choose to make it available to promote interoperability and broaden the market, or choose not to share it.

A growing number of standards require a demonstration of conformance. A *performance standard* states requirements in terms of required results with criteria for verifying conformance, but without stating the methods for achieving required results. Examples of performance standards are the Federal Information Security Management Act (FISMA) and the Health Insurance Portability and Accountability Act (HIPAA). A *prescriptive standard* specifies design requirements, how a requirement is to be achieved, or how an item is to be constructed, but without criteria for measuring the conformity of the results with specified requirements. An example of a prescriptive standard is ISO/IEC 7810 on identification card physical construction. The development and use of performance standards are encouraged since they are less likely than prescriptive specifications to stand in the way of innovation. Still, prescriptive standards are sometimes more appropriate, particularly for describing test methods or procedures or for defining standards to achieve interoperability.

1.2 Cyber Security Standards Interaction

A standard is rarely applied in isolation. When technologies, processes, and management practices are combined to solve a business problem, multiple standards normally come into play. When components are integrated, each may entail one or more technical or management standards. For example, a given business solution is likely to involve a variety of IT security configuration standards, such as networking, communications, and security management standards. Each standard imposes requirements that may or may not conflict with the requirements of other standards.

Standards can interact in several ways. Some standards are *complementary*, which means that one standard supports or reinforces the requirements of another. For example, ISO frequently publishes multipart standards that can be considered complementary, where each part is a separately developed volume covering a different aspect of a central issue. Some standards may *conflict* with each other, which means that there are inconsistencies or contradictions between standards, resulting in issues such as technological incompatibility or legal noncompliance. Other standards are *discrete*, which means that they have no direct effect on one another. There are also *standards gaps*, where there is no formal standard developed for a particular area of security, although a guideline may exist. Standards gaps typically occur when a technology is evolving so rapidly that standards development cannot keep pace. In other cases, a gap exists because consensus has not been reached on either the technology or the standard.

1.3 Standards and Guidelines

Standards can be contrasted with another category of documents, generally referred to as *guidelines*. Both standards and guidelines provide guidance aimed at enhancing cyber security, but guidelines usually lack the level of consensus and formality associated with standards. Some standards, such as ANSI Standards and FIPS Publications, are easily recognized because they include the term *standard* in their titles. Others are harder to recognize. For example, standards issued by the International Telecommunications Union (ITU), an international standards developer, are designated as *Recommendations*. A standard issued by the IETF starts out as an *RFC* and retains that designation even after being adopted as a standard. In other cases, documents that are not standards in the strict sense of the word may be treated as such by an organization if it suits the organization's needs. For example, many US and international organizations and businesses have adopted National Institute of Standards and Technology (NIST) Special Publications as standards, even though those documents are published as guidelines for use by US Federal agencies.

Some organizations develop both standards and guidelines. For example, in addition to international standards, ISO/IEC issues several types of guidelines, including technical specifications, publicly available specifications (PAS), and technical reports, according to the ISO/IEC Directives, Part 1, Section 3 [7]. A technical specification may be published when the immediate release of an international standard is not feasible, such as when the subject in question is still under development. A PAS may be an intermediate specification published prior to the development of a full international standard, or in International Electrotechnical Commission (IEC) it may be a "dual logo" publication published in collaboration with an external organization. A PAS does not fulfill the

requirements for a standard. A technical report is an informative document generally intended to educate the reader, not to specify an international standard.

2 Cyber Security Standards Developers

International, regional, national, industry, and government groups are involved in the development of cyber security standards. An *SDO* is an organization whose primary mission is the development of voluntary consensus standards on an international, regional, or on a national basis. Most SDOs cover a wide variety of technical areas, not just cyber security. *Consortia*, *industry alliances*, and *associations* are all groups of organizations or individuals with similar interests that promote standards development. A consortium is typically formed for a limited time to achieve a specific goal, such as the development of standards. *Industry alliances* and *associations* tend to be more loosely formed to foster common interests. Consortia and industry alliances comprise companies, and associations are made up of individuals. Finally, the US *government* and other national governments develop standards specifically intended for government audiences. Examples of organizations in each of these categories are provided below, along with brief discussions of some of the organizations' cyber security standards work.

2.1 International Standards Development Organizations

The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) develops standards in many areas, including information technology, telecommunications, and power generation. An example of IEEE-SA's security work is its 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee. Various working groups within the committee develop widely used standards for many types of networking technologies, such as Ethernet, wireless LANs, Bluetooth, and Worldwide Interoperability for Microwave Access (WiMAX). These standards include the security features built into the wireless networking protocols.

The IETF is concerned with the evolution of the Internet architecture and the operation of the Internet. The IETF has dozens of working groups that each focus on a different element of the Internet, including several groups working on Internet security. Topics addressed by these working groups include Domain Name System (DNS) security, authentication protocols, routing protocol security, Internet Protocol (IP) version 6, public key infrastructure, e-mail security, event logging, and network traffic encryption.

ISO, whose membership consists of the national standards institutes of more than 150 countries, addresses all standards except those for electrical and electronic engineering, which are the responsibility of the IEC. ISO and IEC formed the Joint Technical Committee 1 (JTC1) for IT standards development, including standards for the security of systems and information. JTC1 has a number of subcommittees (SC) and working groups that address specific technologies. For example, the SC17 group addresses identification cards and personal identification, the SC27 group focuses on IT security techniques, the SC31 group works on automatic identification and data capture (AIDC) techniques, and the SC37 group develops biometric standards.

The ITU-T produces standards, called *Recommendations*, for telecommunication networks. ITU-T's standards are developed by study groups (SG) such as SG17, which covers security, languages, and telecommunications software. SG17 led the development of the ICT Security Standards Roadmap, which provides information on previous and current security standards work from several major standards developers, including ISO, IEC, IETF, Organization for the Advancement of Structured Information Standards (OASIS), Institute of Electrical and Electronics Engineers (IEEE), and telecommunications-specific organizations. It also lists current security standards gaps and provides pointers to security glossaries. SG17 developed the ICT Security Standards Roadmap in collaboration with the European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG).

2.2 Regional Standards Development Organizations

The European Telecommunications Standards Institute (ETSI) produces telecommunications standards within Europe. ETSI's cyber security standards activities include work on electronic signatures, smart cards, lawful interception, and 3GPP.

The CEN, whose members are the national standards organizations of 30 European countries, develops cyber security standards on its own and in conjunction with other international, national, and government standards developers.

2.3 National Standards Development Organizations

In the narrowest sense of the term, ANSI is not an SDO, since it does not develop standards; rather, it administers and coordinates the activities of the US private sector voluntary standardization system. ANSI sponsors cyber security-related working groups, such as a Homeland Security Standards Panel and a Healthcare Information Technology Standards Panel.

The InterNational Committee for Information Technology Standards (INCITS) is an ANSI-accredited organization, which develops US standards for information and communications technologies. INCITS comprise technical committees (TCs) that create standards for different technology areas. Examples of cyber security-focused TCs are B10 (identification cards and related devices), CS1 (cyber security), M1 (biometrics), and T6 (radio frequency identification (RFID) technology).

2.4 Consortia, Industry Alliances, and Associations

The Association for Automatic Identification and Mobility (AIM) is a trade association for entities that are interested in AIDC technologies. AIM performs the development of cyber security standards in areas such as barcodes, card technologies, electronic article surveillance, RFID, real-time locating systems (RTLS), and other AIDC-related technologies.

The British Security Industry Association (BSIA) is the professional trade association for the security industry in the United Kingdom. The BSIA develops codes of practice and technical documents and submits some of them for consideration as British Standards. Security areas addressed by the BSIA include access control, information destruction, physical security equipment, and security systems.

The Information Systems Audit and Control Association (ISACA) is an organization for information assurance, governance, security, and audit professionals. It is best known for its information system auditing and control standards and related initiatives. For example, ISACA has developed Control Objectives for Information and related Technology (COBIT), which is a control framework that encompasses several aspects of IT governance, including risk assessment. COBIT is based on various international standards and can be used to identify appropriate standards references during audits.

The Instrumentation, Systems, and Automation Society (ISA) is a professional association that develops standards for automation technologies. For example, its SP99 working group develops security standards for manufacturing and control systems, such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). Some of ISA's reports on this topic have become ANSI standards.

The OASIS develops standards for security and e-business, and is well known for its web services standards work. OASIS has several working groups focused on security topics such as biometrics, digital signature services, enterprise key management infrastructures, public key infrastructure adoption, and web services security.

The SIA is an ANSI-accredited SDO that develops systems integration and equipment performance standards. Several SIA working groups develop physical security standards on topics such as biometrics, mobile security devices, credential readers, security communications, and security control panels.

2.5 US Government Standards Developers

NIST develops security standards for US Federal information systems. NIST's FIPS have been made mandatory for federal use. Examples of FIPS include FIPS 200, which specifies minimum security requirements for federal information systems; FIPS 199, which provides standards for security categorization of federal systems; and FIPS 197, which defines the Advanced Encryption Standard (AES). NIST also hosts the National Center for Standards and Certification Information (NCSCI), which provides information on US standards and technical regulations, as well as other national, regional, and international standards.

The Office of Management and Budget (OMB) assists the President of the United States in the development of budget, management, and regulatory policies. OMB's products include OMB Circulars and OMB Memoranda, which are instructions or information issued to federal agencies. Some of these documents mandate the use of particular security standards or require federal agencies to meet other security requirements. For example,

OMB Circular A-130 pertains to the management of federal information resources, and OMB Memorandum M-07-16 mandates security controls to protect the confidentiality of personally identifiable information.

3 Getting Involved in Standards Development

In addition to those mentioned above, there are many other cyber security standards developers already working on creating new standards. The ICT Security Standards Roadmap provides information on a number of ongoing standards activities. Organizations interested in cyber security standards development can join existing standards efforts so that they can ensure that standards are developed in a way that is favorable to, or at least compatible with, their critical interests.

In addition to influencing the direction that a standard takes, actively participating in the standards development process offers other advantages. An organization gains a better understanding of the standards under development, their underlying designs, the trade-offs and compromises made during their development, and the operating conditions and environments they are intended to serve. Organizations make contacts and build relationships with technical experts involved in the development effort, as well as improving their own technical knowledge. Participation in standards development also benefits the security community by sharing the effort across many organizations.

Most organizations do not participate in standards development activities. They may feel that it is not important, that it is impossible to influence the outcome, or that involvement is too expensive. Nevertheless, participation can be critical to realizing the benefits of standards. Also, organizations that choose not to get involved can find themselves faced with new standards with which they are not prepared to comply.

There are a number of ways to participate in the standards development process, each with its own level of resource commitment. Organizations can choose how fully to participate, depending upon the importance of the standard to the organization and the resources they have available to commit to the effort. *Trackers* follow the development of a standard at a high level, for example, by reading summaries and implementation timelines on the developer's public website. Tracking the progress of a new standard gives organizations the ability to anticipate its effects, even if they choose not to become more actively involved in its development. *Public reviewers* review drafts of the standard and submit comments, which can influence the content and impact of a standard under development. For particularly important standards, organizations should consider becoming *members* of the entity developing the standards.

The role of *driver* may be appropriate when the organization's stake in a new standard is critical. It may be that producing the standard is part of the organization's charter or mission; driving the development of a standard may require significant resources.

In addition to contributing to the development of new standards, organizations should also consider participating in the maintenance of existing standards. Most standards undergo periodic review and revision. SDOs typically have established formal maintenance programs to help ensure that their standards do not become dated due to technological evolution, changes to related standards, or other causes.

References

1. International Organization for Standardization/International Electrotechnical Commission (2004). *ISO/IEC Directives Part 2:2004 (Rules for the Structure and Drafting of international Standards)*, 5th ed., http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/International%20Standardization/ISO/ISOIECDirectivesPart2pdfformat.pdf.

2. National Institute for Standards and Technology (2001). *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, May. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

3. ITU-T, European Network and Information Security Agency (ENISA), Network and Information Security Steering Group (NISSG) (2007). *ICT Security Standards Roadmap*, version 2.2, September 2007. http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.

4. ISO/IEC JTC1/SC27 (2008). *Standing Document 6 (SD6): Glossary of IT Security Terminology*, 2008-03-19. http://www.jtc1sc27.din.de/sce/SD6.

5. Internet Engineering Task Force (2007). *Internet Security Glossary*, August 2007. http://www.ietf.org/rfc/rfc4949.txt.

6. ITU Telecommunication Standardization Sector (2008). *Security Compendium, Part 2—Approved ITU-T Security Definitions*, http://www.itu.int/dmspub/itu-t/oth/0A/0D/T0A0D00000A0001MSWE.doc.
7. ISO/IEC (2008). *ISO/IEC Directives Part 1:2008 (Procedures for the Technical Work)*, 6th ed., http://isotc.iso.org/livelink/livelink/fetch/2000/2122/3146825/4229629/4230450/4230455/ISO IEC Directives Part 1 Procedures for the technical work—2008 6th ed.—PDF format?nodeid=4230504&vernum=0.

Further Reading

American National Standards Institute (ANSI) (2008). *ANSI Standards Activities*, http://www.ansi.org/standardsactivities/overview/overview.aspx?menuid=3.

Association for Automatic Identification and Mobility (AIM) *AIM Global Standards*, http://www.aimglobal.org/standards/.

British Security Industry Association (BSIA) http://www.bsia.co.uk/index.php.

Department of Homeland Security (DHS) http://www.dhs.gov/index.shtm.

European Committee for Standardization (CEN) http://www.cen.eu/cenorm/homepage.htm.

European Network and Information Security Agency (ENISA) http://www.enisa.europa.eu/index.htm.

European Telecommunications Standards Institute (ETSI) *ETSI Standards*, http://www.etsi.org/WebSite/Standards/Standard.aspx.

IEEE, IEEE Standards Association (IEEE SA) http://standards.ieee.org/.

Information Systems Audit and Control Association (ISACA) http://www.isaca.org/Template.

ISO/IEC Joint Technical Committee 001 "Information Technology". http://www.jtc1.org/.

InterNational Committee for Information Technology Standards (INCITS) http://www.ncits.org/.

International Electrotechnical Commission (IEC) http://www.iec.ch/.

Internet Engineering Task Force (IETF) http://www.ietf.org/.

International Organization for Standardization (ISO) http://www.iso.org/iso/home.htm.

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) http://www.itu.int/ITU-T/.

Instrumentation, Systems, and Automation Society (ISA), ISA Standards http://www.isa.org/Template.cfm?Section=Standards2&Template=/customsource/isa/Standards/AutomationStandards.cfm.

National Institute of Standards and Technology (NIST) http://csrc.nist.gov/.

NIST National Center for Standards and Certification Information (NCSI) http://ts.nist.gov/Standards/Information/index.cfm.

Information & Communications Technologies (ICT) Standards Board Network and Information Security Steering Group (NISSG). http://www.ictsb.org/Working Groups/NISSG/index.htm.

Office of Management and Budget (OMB) http://www.whitehouse.gov/omb/.

Organization for the Advancement of Structured Information Standards (OASIS) http://www.oasis-open.org/.

Process Control Systems Forum (PCSF) https://www.pcsforum.org/.

Security Industry Association (SIA), SIA Standards. https://www.siaonline.org/standards/index.html.

United States Computer Emergency Readiness Team (US-CERT), Control Systems Security Program (CSSP) http://www.us-cert.gov/control systems/index.html.

Cross-References

Regulations and Standards
Authentication, Authorization, Access Control, and Privilege Management
Cryptography
Protocol Security
Wireless Security