Applying NIST SP 800-53 to Industrial Control Systems

Stuart Katzke and Keith Stouffer, National Institute of Standards & Technology, Gaithersburg, MD
Marshall Abrams, The MITRE Corporation, McLean, VA
David Norton, Entergy, Inc. New Orleans, LA
Joe Weiss, KEMA, Inc., Cupertino, CA

Keywords: CIP, cyber security, ICS, industrial control system, information security, NERC, NIST, security control

Abstract

The National Institute of Standards and Technology (NIST) has established an *Industrial Control System Security Project* to improve the security of public and private sector Industrial Control Systems (ICSs). A major part of the project is to research the applicability of NIST Special Publication (SP) 800-53 *Recommended Security Controls for Federal Information Systems* to ICSs. SP 800-53 contains specifications for information security[1] controls[2] that are binding on all non-national security information and information systems[3] belonging to, or operated for, federal agencies. SP 800-53 was developed for use with traditional IT systems. Another major part of the project is to clarify and rectify problems experienced in applying SP 800-53 to ICSs.

---

[1] The terms *information security*, *information systems security*, and *cyber security* are used synonymously in this paper as: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. NIST documents primarily use the terms, *information security* and *information systems security*, while the June 2006 North American Reliability Council (NERC) Critical Infrastructure Protection (CIP) standards use the term *cyber security*.

[2] The word *control* has two different uses in this paper: (1) Used as an adjective of "system" (e.g., *control* system, industrial *control* system), it indicates that the system being discussed functions as a real-time process control system (e.g., Supervisory Control and Data Acquisition System–SCADA, Distributed Control System–DCS). (2) Used as a noun (e.g., security *control*), it refers to a management, technical, and operational security safeguard or countermeasure that is implemented in an information system (including real-time process control systems such as SCADA and DCS) to protect the system against information technology-related threats that result in loss of confidentiality, integrity, or availability of the system's function or its information. Readers of this paper are expected to determine which interpretation of *control* is intended based on the context in which the term is used.

[3] An information system is a discrete set of information resources (consisting of information and related resources, such as personnel, equipment, funds, and information technology) organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

 Presented at ISO EXPO 2006 – http://www.isa.org

Although several organizations are working on information security standards and guidelines, at the time this research was conducted, the NERC cyber security standards, CIP 002-1 to CIP 009-1, were the only available documents addressing security controls comparable to those contained in SP 800-53. Therefore, the research focused on comparing the NERC CIP standards with SP 800-53.

A careful analysis of correspondence between SP 800-53 and the NERC CIP standards concluded that an organization conforming to one of the baseline sets of security controls in SP 800-53 can also comply with the management, operational and technical security requirements of the NERC CIPs, though the converse may not be true.

As an active participant in both the information security and ICS communities (government and private sector), NIST is working on harmonizing ICS information security controls within the ICS community. If successful, the results are expected to influence a major portion of the ICS community, including other types of federal ICSs, regulatory agencies, national and international voluntary standards activities, and commercial sector ICSs (e.g., manufacturing processing systems, building control systems).

1 INFORMATION SECURITY IN INDUSTRIAL CONTROL SYSTEMS

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), programmable logic controllers (PLC), and other smaller control system configurations often found in the industrial control sectors. ICSs are used in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries.

Many ICSs in use today were developed years ago, long before public and private networks, desktop computing, or the Internet were a common part of business operations. These systems were designed to meet performance, reliability, safety, and flexibility requirements. In most cases they were physically isolated from outside networks and based on proprietary hardware, software, and communication protocols that included basic error detection and correction capabilities, but lacked the secure communications required in today's interconnected systems. The need for information security measures within these systems was not anticipated, and at the time, security for ICSs meant physically securing access to the network and the devices that controlled the systems.

As microprocessor, personal computer, and networking technology evolved during the 1980's and 1990's, ICS design changed to incorporate the latest information technologies, such as the use of commercial off-the-shelf-products (e.g., Windows operating systems) and open protocols (e.g., TCP/IP). Internet-based technologies started making their way into ICS designs in the late 1990's. These changes to ICSs exposed them to new types of threats and significantly increased the likelihood that they could be attacked.

2 COMPARING INDUSTRIAL CONTROL SYSTEMS AND INFORMATION SYSTEMS

Although ICSs are information systems, until recently they had little resemblance to typical information systems in that they were isolated systems running proprietary control protocols. ICSs generally have more stringent safety, performance and reliability requirements and many were designed with special purpose operating systems and applications that may be considered unconventional when compared with typical information systems. However, as ICSs have been integrated with corporate information systems through increased connectivity and remote access capabilities, they have started to resemble typical information systems. While integration supports new corporate information system capabilities that improve overall enterprise operations and decision making, integration provides significantly less isolation for ICSs from the outside world than predecessor systems, creating a greater need to secure these systems.

While security solutions have been designed to deal with security issues in typical information systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new IT security solutions are needed. This is because 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 risks such as production losses, negative impact to a nation's economy, and compromise of proprietary information. Furthermore, the goals of safety and security sometimes conflict with the operational requirements of ICSs. Since ICSs are pervasive throughout the nation's critical infrastructure, failures or corruption in these systems can result in serious disruptions to the critical infrastructures they support.

3 NIST'S RESPONSIBILITIES FOR THE SECURITY OF ICSs

Through NIST's congressionally assigned responsibility to develop and promulgate security standards and guidelines (S&Gs) for federal information systems, NIST's Information Technology Laboratory (ITL) Computer Security Division (CSD), in cooperation with NIST's Manufacturing Engineering Laboratory (MEL) Intelligent Systems Division (ISD), has the ability to establish information security standards for federally owned/operated ICSs as well as for those ICSs that are operated by contractors on behalf of the federal government.

For example, *The Federal Information Security Management Act (FISMA) of 2002* (http://csrc.nist.gov/policies/FISMA-final.pdf) places significant requirements on federal agencies for the protection of information and information systems; and places significant requirements on the National Institute of Standards and Technology (NIST) to assist federal agencies in complying with FISMA, including the development and promulgation of information security S&Gs.

FISMA required NIST to develop two mandatory Federal Information Processing Standards (FIPS) that apply to all federal information and information systems, including ICSs. These standards are: (i) FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*; and

(ii) FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. FIPS 199 is a standard for determining the security category of an information system. FIPS 199 security categories (low, moderate, and high) are based on the potential impact on an organization should certain events occur which jeopardize the information and information system needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FIPS 200 is a standard that specifies mandatory minimum security requirements all federal information systems must meet, including ICSs.

To support both FIPS 199 and 200, NIST developed Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. SP 800-53 requires federal agencies to implement one of three minimum (baseline) sets of security controls for every information system in the agency based on the systems' security categorization. The baselines were constructed from the security controls listed in the control catalogue that is also contained in SP 800-53. While FIPS 199, FIPS 200, and SP 800-53 apply to the federal government's non-national security systems, these S&Gs were developed with the recognition that, on occasion, sector-specific interpretations of the SP 800-53 security controls may have to developed for various reasons (e.g., sector-specific laws/regulations/policies, sector-specific technologies, sector-specific application/performance requirements). For ICSs, federal agencies identified a need to clarify the requirements and rectify problems experienced in applying SP 800-53 security controls.

4 THE NIST INDUSTRIAL CONTROL SYSTEM SECURITY PROJECT

As a proof-of-concept that FIPS 199, FIPS 200, and SP 800-53 can be interpreted and applied to the ICS sector, NIST's Computer Security Division (CSD) and Intelligent Systems Division (ISD) initiated a *joint Industrial Control System Security Project* in January 2006. The objective of this project is to work cooperatively with federal sector stakeholders in the ICS area, and where needed, to craft an interpretation of the SP 800-53 security controls for ICSs. As part of the joint ICS project, NIST is also developing SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security* that addresses vulnerabilities, threats, and security controls in the context of information system security program development and deployment.

NIST recognizes that the development of security control standards for federally owned/operated ICSs must be accomplished in cooperation and coordination with the many on-going industry standards activities such as the North American Electric Reliability Council (NERC) Cyber Security Standards for Critical Infrastructure Protection (CIP), CIP-002-1 through CIP-009-1, ISA SP99 *Manufacturing and Control Systems Security* standard and the IEC 62443 *Security for Industrial Process Measurement and Control – Network and System Security* standard. Consequently, this project proposes to examine the different security control solutions and/or standards being developed within the ICS community and, based on this examination and on the FIPS 200/SP 800-53 foundation that has already been established for federal agencies, develop a candidate set of security requirements and baseline security controls that will apply to all federal ICSs. This project will use an open public process in developing its candidate set of security requirements and baseline security controls that aggressively seeks inputs and comments from all stakeholders (i.e., government, industry, and academe). Once the candidate security requirements and associated security controls have been developed for the federal government, NIST will recommend their adoption by the federal ICS community. Since the candidate security requirements and controls will have gone through an extensive open, public vetting process during their development, NIST will work within the private sector ICS community to foster convergence on the security requirements and security controls that have been adopted for federal ICSs. For example, as a member and a technical editor of the committee developing the ISA-SP99 standard, and a member of the committee developing the IEC 62443 standard, NIST ISD staff is working within these organizations to facilitate the development of common ICS security control standards. A vehicle under consideration to harmonize the security requirements for the various industry standards is the formation of a Security Requirements Interest Group under the Department of Homeland Security (DHS) Process Control Systems Forum (PCSF) (https://www.pcsforum.org).

5 APPLYING SP 800-53 TO ICSs

NIST Special Publication 800-53 provides a rich set of security controls that satisfy the breadth and depth of security requirements levied on information systems and that are consistent with, and complementary to, other established security standards. The catalog of security controls contained in SP 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. Security controls are the management, operational, and technical safeguards and countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

NIST researched how well SP 800-53 addresses information security in ICSs, with particular focus on electric energy systems that are part of the nation's critical infrastructure. As part of this research, federal agency ICS stakeholders participated in an *ICS Workshop* held at NIST on April 19-20, 2006. Some of the findings of the research will be incorporated into the 2006 annual revision of SP 800-53 (i.e., SP 800-53, Rev 1). Work on other findings is continuing and is expected to be reflected in future revisions to SP 800-53.

A key aspect of the research was to determine how the SP 800-53 security controls correspond to the set of NERC Cyber Security Standards for Critical Infrastructure Protection. At the time this research was conducted, the NERC CIP standards were the only available documents addressing security controls comparable to those contained in SP 800-53. The NERC CIP standards are assumed representative of concerns in one sector of the ICS community (i.e., the electricity sector). The insights gained from this comparison have proven to be valuable to NIST and will benefit the ICS community.

On July 20, 2006, the U.S. Federal Energy Regulatory Commission (FERC) approved the North American Electric Reliability Council's (NERC) application to become the Electric Reliability Organization (ERO) for the United States. As the ERO, NERC will have legal authority to enforce reliability standards on all owners, operators, and users of the bulk power system, rather than relying on voluntary compliance. Once enforced, Federal agencies that own or operate systems that are part of the bulk power system will have to meet the requirements of the NERC CIP standards and FIPS 200/NIST SP 800-53.

6 THE NERC CIP STANDARDS

Presidential Decision Directive 63 (PDD-63), "Protecting America's Critical Infrastructures", officially identified "electricity" as a critical infrastructure and designated NERC as the Sector Coordinator for the Electricity Sector. PDD-63, and the later Homeland Security Presidential Directive – 3 (HSPD-3), calls for a framework for cooperation within individual infrastructure sectors and with government, for the vital mission of protecting critical infrastructures. NERC, as the Electricity Sector Coordinator, has the responsibility to:

- assess sector vulnerabilities;
- develop a plan to reduce electric system vulnerabilities;
- propose a system for identifying and averting attacks;
- develop a plan to alert electricity sector participants and appropriate government agencies that an attack is imminent or in progress; and
- assist in reconstituting minimum essential electric system capabilities in the aftermath of an attack.

The NERC CIP standards were developed in this context with applicability to electric infrastructure systems, including:

- balancing authorities;
- generator owners and operators;
- interchange authorities;
- load-serving entities;
- offices of NERC;
- regional reliability organizations;
- reliability coordinators; and
- transmission owners and operators.

Certain entities were excluded from the coverage of the NERC CIP standards:

- communication networks and communication;
- facilities regulated by the U.S. Nuclear Regulatory Commission and the Canadian Nuclear Safety Commission; and
- links between discrete Electronic Security Perimeters.

7 COMPARING NIST SP 800-53 CONTROLS AND NERC CIP STANDARDS

Comparing control sets produced by different organizations with different frameworks is difficult and subject to interpretation. While the mapping discussed below represents a significant effort by a number of experts from both the ICS and information security communities working together, there are no guarantees that the mapping is completely accurate or correct. This is due to the significant subjectivity that occurs when performing these types of mapping exercises. However, while not perfect, the authors of this paper were confident that the mapping was good enough to make comparisons between the two sets of standards and draw some conclusions. The conclusions are stated below in the *Conclusion and Future Directions Toward Harmonization* Section of this paper.

SP 800-53 has 17 families of information (i.e., cyber) security controls. The NERC CIP standards (CIP 002-009) often addressed more than one SP 800-53 family; therefore the NERC CIP standards generally correspond to controls in one or more of the SP 800-53 control families. In general:

- Most *requirements* in the NERC CIP correspond to *controls* in SP 800-53.
- *Measures* in the NERC CIP are used to demonstrate (i.e., measure) compliance with NERC CIP requirements. NERC CIP *Measures* correspond to *assessments* of the security controls in SP 800-53 (i.e., determination of the overall effectiveness of controls; that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). Within NIST's FISMA-related document suite, security control assessments are described in SP 800-53A: *Guide for Assessing the Security Controls in Federal Information Systems*.
- *The compliance* concept in the NERC CIP standards is CIP standard-specific. There is a compliance component in each CIP standard that defines the key roles and the criteria for complying with the specific CIP standard. Compliance is intended to provide confidence that the requirements of the specific CIP standard have been and continue to be met on a periodic basis; and that the documentation requirements have been met for the CIP standards. Compliance with a specific CIP standard has no direct analogue in the NIST set of documents.

The remainder of this paper focuses on the differences that exist between the two sets of standards.

7.1 THE MAPPING: ROW AND COLUMN COUNTS

Table 1 is the first page of the complete mapping between SP 800-53 and the NERC CIP standards. The first page is included here only for the purpose of illustrating how to interpret the full mapping. The full mapping will be available at http://csrc.nist.gov/sec-cert/.

SP 800-53 identifies the minimum security controls, or security control baselines, for low-impact, moderate-impact, and high-impact information systems. Table 1 employs shading to identify where each security control fits in the control baseline.

Note that Table 1 contains a count of the number of entries in each row and column. This count shows the number of table entries for each NERC CIP requirement and each SP 800-53 control. This count is a very useful indication of the correspondence between the two documents and the distribution, or spread, of that correspondence. Some Count cells reflect a higher number than the entries marked in the respective row or column due to the fact that the table was "trimmed" to fit this document.

Addressing the SP 800-53 controls in the rows of the table first, note that a zero count indicates that there is no corresponding NERC CIP requirement. A count of one indicates that there is a unique relationship between the SP 800-53 control and the corresponding NERC CIP requirement. Looking across the row, you can find that correspondence. The numeric code for the correspondence is explained in Section 7.2 below. The actual NERC CIP requirement is found by looking at the column heading. A number larger than one indicates the number of NERC CIP requirements that correspond to the 800-53 control. Looking across the row, you can find those correspondences. The numeric codes for the correspondences are explained in

Table 1. Mapping Between SP 800-53 and NERC CIP (first page)

			CIP-002				CIP-003						CIP-004				CIP-005				
LEGEND High baseline (no shading) Moderate baseline (12.5% grey shading) Low Baseline (25% grey shading) No Baseline (50% grey shading) NERC CIP FINAL			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance
Other - Notes							3		11	2	2, 7										
SP 800-53 Rev. 1 Controls		Count	4	4	3	3	19	3	2	9	4	5	4	6	4	9	5	12	7	7	5
Access Control																					
AC-1	Access Control P & P	4					8				8							13			
AC-2	Account Management	3									13					17					
AC-3	Access Enforcement	0																			
AC-4	Information Flow Enforcement	0																			
AC-5	Separation of Duties	0																			
AC-6	Least Privilege	3														17					
AC-7	Unsuccessful Logon Attempts	0																			
AC-8	System Use Notification	1																8			
AC-9	Previous Logon Notification	0																			
AC-10	Concurrent Session Control	0																			
AC-11	Session Lock	0																			
AC-12	Session Termination	0																			
AC-13	Supervision and Review—A C	0																			
AC-14	Permitted Actions without I or A	0																			
AC-15	Automated Marking	0																			
AC-16	Automated Labeling	0																			
AC-17	Remote Access	3															12	9	8		
AC-18	Wireless Access Restrictions	3															7	17	17		
AC-19	Access Control for Portable and Mobile Systems	2																17	17		
AC-20	Personally Owned Information Systems	0																			
Awareness and Training																					
AT-1	Security Awareness and Training P & P	3					3						13	13							
AT-2	Security Awareness	1											8								
AT-3	Security Training	1												8							
AT-4	Security Training Records	1												8							
AT-5	Contacts with Security Groups & Associations	0																			

Section 7.2 below. The actual NERC CIP requirements are found by looking at the column heading of each correspondence. A large number in the row count (say greater than or equal to 5) indicates that the SP 800-53 control is addressed in a large number of NERC CIP requirements. In general, SP 800-53 addresses

related NERC CIP requirements within a control family, while the SP 800-53 controls are distributed over multiple NERC CIP standards.

Looking at the NERC CIP requirements in the columns of the table, the counts have a similar interpretation to the row counts. A large number in a (NERC CIP requirement) column count indicates that the NERC CIP requirement overlaps with multiple SP 800-53 controls.

High row and column counts are indications of the challenges in comparing documents since that means the mappings are "many-to-many".

7.2 MAPPING CODES

Gradations in the degree of correspondence between SP 800-53 controls and NERC CIP standards are captured in the code numbers detailed below (i.e., the codes are used to convey more than just the presence of a correspondence). These codes are used in the row-column entries in Table 1. Additional information about the nature of the correspondences is indicated by the mapping codes contained in the "Other Notes" row of Table 1.

The meaning of the mapping codes appearing in Table 1 are as follows:

2 NERC requirements include management responsibilities that are outside the scope of SP 800-53.
3 The NERC requirement has broader scope than the corresponding SP 800-53 control and may cover multiple SP 800-53 controls as well as controls not in SP 800-53.
7 The subheading of the NERC requirement corresponds to a SP 800-53 security control. This NERC requirements subheading is more encompassing in its scope than the corresponding SP 800-53 security control.

8 NERC requirement and SP 800-53 security controls are essentially equivalent.
9 NERC requirements are more specific than SP 800-53 security control.
11 NERC requirement has no counterpart in SP 800-53.
12 Both NERC requirements and SP 800-53 security control contain specifics not found in the other.
13 NERC requirement addresses a subset of the SP 800-53 security control.
17 NERC requirement is less specific than the corresponding SP 800-53 security controls.

8 CONCLUSIONS AND FUTURE DIRECTIONS TOWARD HARMONIZATION

A careful analysis of the correspondences between SP 800-53 controls and the NERC CIP standards concluded that an organization conforming to the baseline sets of security controls in SP 800-53 will also comply with the NERC CIP requirements that fall into the category of (i.e., map to) management, operational, and technical controls.

However, NERC contains requirements that fall into the category of "business risk reduction". These are high level business-oriented requirements intended to demonstrate the enterprise is practicing "due diligence" in reducing overall business risk. The evidence/records that result from these requirements are intended to be used in the event of an enterprise cyber security audit. SP 800-53 does not contain analogues to these types of requirements as SP 800-53 focuses on information security controls (i.e., management, operational, and technical) at the information system level.

Federal agencies that own, operate, and maintain ICSs must comply with NIST information security standards and guidelines. Prior to the work reported herein, there has been no serious effort to ensure that the cyber security standards and best practices emerging from the electric power industry are consistent with the federal standards and guidelines being developed by NIST in response to the Federal Information Security Management Act (FISMA). Trying to conform to multiple requirements is difficult. When there is conflict, the difficulty escalates. For example, Federal agencies that own or operate electric energy transmission and distribution systems must comply with SP 800-53 and, depending upon Federal Energy Regulatory Commission (FERC) regulations, may come under other regulatory mandates that could potentially conflict with NIST S&Gs.

NIST plans to continue working with the federal ICS stakeholders, including FERC, Department of Homeland Security (DHS), Department of Energy (DOE), the national laboratories, and federal agencies that own, operate, and maintain ICSs, to develop an interpretation of SP 800-53 for ICSs that permits real and practical improvements to the security of ICSs and, to the extent possible, ensures compliance with the management, operational, and technical requirements in the NERC CIP standards. While private sector ICSs are generally not required to meet NIST's S&Gs (unless they are under contract to a federal agency), they may voluntarily adopt NIST S&Gs if they find them appropriate.

In the private sector, there are many activities currently ongoing to develop ICS cyber security standards. There are industry specific, cross-industry, and international efforts.

NIST recognizes that many ICS sector organizations may wish to migrate towards uniform standards and guidelines along their sector specific interests. The historical, technical, and regulatory reasons for these sector specific interests is beyond the scope if the paper. NIST is actively engaged with the various ICS communities to achieve harmonization and convergence of ICS standards development activities including: participation in the 2006 International Control Systems Security and Standards Coordination Workshop held August 10-11 in Portland, Oregon; participation as a committee member and a technical editor in the committee developing the ISA-SP99 standard; participation as a committee member in the committee developing the IEC 62443 *Security for Industrial Process Measurement and Control – Network and System Security* standard; and collaborations with DHS, DOE, FERC, the national laboratories and federal agencies that own, operate, or maintain ICSs.

One way to move towards convergence is for all stakeholders to use the same terminology and to eliminate duplicative or overlapping control sets. NIST has a set of publications addressing most of the relevant managerial, administrative, operational, procedural, and technical considerations. Each of these publications, such as SP 800-53, have been put through a significant public vetting process by all sectors, including, to the extent possible, by authorities in the national security domain. NIST offers its documents to all organizations interested in using them as a basis for developing common standards within the ICS community.

BIBLIOGRAPHY

Federal Information Security Management Act of 2002 (FISMA). http://csrc.nist.gov/policies/FISMA-final.pdf

Standards for Security Categorization of Federal Information and Information Systems, National Institute for Standards and Technology, FIPS 199, February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Minimum Security Requirements for Federal Information and Information Systems, National Institute for Standards and Technology, FIPS 200 , March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Recommended Security Controls for Federal Information Systems, National Institute for Standards and Technology, SP 800-53 revision 1 (draft), July 2006. http://csrc.nist.gov/publications/drafts/800-53-rev1-clean-sz.pdf

Guide for Assessing the Security Controls in Federal Information Systems, National Institute for Standards and Technology, SP 800-53A (draft), April 2006. http://csrc.nist.gov/publications/drafts/Draft-SP800-53A-spd.ZIP

North American Electric Reliability Council, Critical Infrastructure Protection Standards, June 2006

- CIP-002-1 *Critical Cyber Asset Identification*. ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-002-1.pdf
- CIP-003-1 *Security Management Controls*. ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-003-1.pdf
- CIP-004-1 *Personnel & Training*. ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-004-1.pdf
- CIP-005-1 *Electronic Security Perimeter(s)*. ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-005-1.pdf
- CIP-006-1 *Physical Security of Critical Cyber Assets*. ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-006-1.pdf
- CIP-007-1 *Systems Security Management*. ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-007-1.pdf
- CIP-008-1 *Incident Reporting and Response Planning*. ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-008-1.pdf
- CIP-009-1 *Recovery Plans for Critical Cyber Assets*. ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-009-1.pdf

SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, National Institute for Standards and Technology, SP 800-82 (draft), expected August 2006.

ORGANIZATIONS

National Institute for Standards and Technology (NIST), FISMA Implementation Project. http://csrc.nist.gov/sec-cert/

International Society for Measurement and Control (ISA), Manufacturing and Control Systems Security Project, ISA-SP99. http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

International Electrotechnical Commission Project : IEC 62443, SECURITY FOR INDUSTRIAL PROCESS MEASUREMENT AND CONTROL - Network and system security. http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=62443&part=&se=&submit=Submit

US Federal Energy Regulatory Commission (FERC) Electric Reliability. http://www.ferc.gov/industries/electric/indus-act/reliability.asp#skipnavsub

ACRONYMNS

DCS	Distributed Control Systems
DHS	Department of Homeland Security
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ICS	Industrial Control Systems
NERC	North American Electric Reliability Council
NIST	National Institute of Standards and Technology
PCSF	Process Control Systems Forum
PLC	Programmable Logic Controller
S&Gs	Standards and Guidelines
SCADA	Supervisory Control and Data Acquisition