EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cybersecurity Procurement Benchmark

1023502

Cybersecurity Procurement Benchmark

1023502

Technical Update, August 2011

EPRI Project Manager

R. Austin

This document does **NOT** meet the requirements of
10CFR50 Appendix B, 10CFR Part 21,
ANSI N45.2-1977 and/or the intent of ISO-9001 (1994)

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Southern Engineering Services, Inc.

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

Southern Engineering Services, Inc.
331 Allendale Drive
Canton, GA 30115

Principal Investigator
Bradley Geddes

This report describes research sponsored by EPRI. EPRI would like to acknowledge the support of the following personnel who contributed to this report:

Nick Alexander, British Energy
Janardin Amin, Luminant
Steve Batson, CISSP, Invensys Critical Infrastructure and Security Practice
James P. Batug, PPL Generation, LLC
Matthew Bohne, GE-Hitachi Nuclear Energy (GEH)
Vic Fregonese, AREVA
Bruce Geddes, Southern Engineering Services
Jan Geib, SCANA
William Gross, NEI
Curt Jensen, DN2K
Billy Owen, Energy Northwest
James Pritchett, Progress Energy
Ted Quinn, Technology Resources
Ernie Rakaczky, Invensys Operations Management (IOM)
Pat Samples, Mitsubishi Nuclear Energy Systems, Inc.
Jim Shank, PSE&G, Salem/Hope Creek
Graham Speake, Yokogawa
Kevin Staggs, Honeywell
Chris Sterba, Omaha Public Power District
Thomas Stevenson, Constellation Energy
Lawrence Tremonti, DTE Energy
Deborah Williams, INPO

Stephen Hesler, EPRI
Aaron Hussey, EPRI
Annabelle Lee, EPRI
Erfan Ibrahim, EPRI
Letitia Midmore, EPRI
Joseph Naser, EPRI
Galen Rasche, EPRI

This publication is a corporate document that should be cited in the literature in the following manner:

Cybersecurity Procurement Benchmark. EPRI, Palo Alto, CA: 2011. 1023502.

ABSTRACT

New and replacement instrumentation and control (I&C) systems have significant digital features and functions that require the application of cybersecurity technical and programmatic controls in order to ensure their continued availability in critical systems. Such systems are subject to cybersecurity regulations and standards. Without detailed guidance on how to specify and manage the application cybersecurity controls from system vendors in the procurement process, utilities face the potential for costly rework during the course of a capital project or after a system is implemented.

This report documents the Phase 1 activity of a project to develop guidance for assisting utilities in the specification and management of cybersecurity technical and programmatic controls in order to reduce the risk of costly backfit to new I&C digital equipment in order to meet cybersecurity commitments.

This report is a qualitative benchmark intended to determine the standards, guidance, and practices currently in use in a variety of industries for specifying appropriate cybersecurity requirements for new digital I&C equipment. These benchmark results will be used in developing the scope of the overall project follow-on phases for developing cybersecurity procurement guidance for digital I&C systems that are designated as critical assets (and, therefore, must be protected from postulated cyber threats).

Keywords
Critical assets
Critical digital assets
Cybersecurity guidance
Cybersecurity procurement
Cybersecurity standards

CONTENTS

1
INTRODUCTION AND SUMMARY

1.1 Project Overview: Phase 1 – Cybersecurity Procurement Requirements Benchmark

The overall project objective is to develop generic instrumentation and control (I&C) digital systems cybersecurity procurement guidance for critical assets along with specific procurement language with worked examples. The intended uses of the guidance are to assist utilities with procurement of I&C components and systems and reduce the risk of costly rework when a system is implemented. The stated goal for the entire project is to assist utilities in preventing costly backfit to new digital equipment in order to meet cybersecurity commitments.

The purpose of Phase 1 is to perform a limited set of interviews with a cross section of various entities including nuclear and nonnuclear utilities, I&C vendors, and others in order to capture existing procurement standards, guidance, and practices for digital systems. Appendix A contains the benchmark interview questionnaire. Appendix B contains a list of type of companies, industries, and roles of persons interviewed and, where approved, the name of the company and person interviewed.

This benchmark study has been created based on the results of the interviews to determine whether existing standards, guidance, and/or practices are in use that EPRI can recommend or whether additional work is required to develop guidance for procurement of I&C digital systems that are intended for use as critical assets. If additional work is required, EPRI will use existing best practices to inform its work.

1.2 Benchmark Approach and Summary

Interviews were performed by various members of the project team and were documented using the benchmark questionnaire (see Appendix A). The completed questionnaires are retained in the project file. Only a summary of the questionnaire results is presented in this technical update. Most of the “comments” are paraphrased and are not direct quotes. Many comments are a summary of a detailed verbal discussion, and most interviewees did not fill out the questionnaire. When multiple interviewees made the same basic point, a single paraphrased comment was created. The bases for selection and paraphrasing of interviewee statements were that 1) they were related to the question (vendors, in particular, often provided additional detail and insight beyond the scope of question) and 2) many interviews tended to be lengthy, detailed discussions, and it was most expedient to paraphrase them into a condensed form. Some interviewees identified additional cybersecurity standards and guidance documents or development projects. When possible, the project team performed research on these additional items or identified additional individuals for interviews.

Phase 1 was **not** intended as an exhaustive quantitative research effort to discover and document all of the standards and guidance available for digital I&C systems cybersecurity. Rather, the intent was to look for qualitative information in an effort to characterize available standards and good practices and to benchmark the existing standards, guidance, and/or practices that are used in a variety of industries and entities as well as to identify gaps between those and actual needs for I&C system cybersecurity procurement guidance.

1.2.1 Summary of Sample Cross Section

A cross section of organizations contributed to the project. In some cases, the interviewee directed the project team to investigate other standards or projects. These investigations, in some cases, did not involve additional interviews; however, the results of the investigation are included. The following are representative categories included in the study:

- Nuclear utilities
- Nuclear I&C vendors
- Fossil generation utilities
- Nonnuclear I&C vendors
- New nuclear plant nuclear steam supply systems (NSSS) vendors
- Industry organizations such as Nuclear Energy Institute (NEI) and International Electrotechnical Commission (IEC)
- Independent consultants and consulting organizations
- Non-utility critical asset monitoring and management vendors
- Financial institutions

1.2.2 Summary of Standards or Guidance in Use or Planned for Use

Cybersecurity for I&C digital systems that comprise critical assets within the entire generation, transmission, and distribution infrastructure in every country is a high priority. Many regulatory agencies, standards bodies, industry organizations, governmental agencies, and user groups are actively addressing this issue in a variety of ways. A list of those documents and activities identified by the interviewees is included in Section 3.

1.2.3 Summary of Actual Practices

Actual practices vary from buyer to buyer and vendor to vendor; they do not follow any consistent pattern, with some exceptions in non-utility I&C procurement activities. A few utility buyers have developed some procurement guidance. Most utility buyers ask for compliance with a cybersecurity standard such as NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors,” ISA-99, “Industrial Automation and Control Systems Security,” or North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) NERC-CIP-002-009, “Cyber Security – Critical Cyber Asset Identification” (see Sections 3.2 and 5 for a complete description of standards references), listing general requirements from the standard, with little tailoring to the project needs [1, 2, 3].

Commercial and nonnuclear buyers are developing a pattern of using the U.S. Department of Homeland Security (DHS) or Working-party on Instrument Behavior (WIB) procurement guidance as a reference or guide that is tailored to their specific project, although this is not consistent. The vendors are responding favorably to the use of the DHS guidance; some report that the WIB guidance is more prescriptive and costly.

International Society of Automation (ISA) has developed a program to certify a vendor component or system to ISA-99 known as ISASecure. Some vendors have decided to spend the resources to obtain this certification. If the procurement standard references ISA-99, an ISASecure vendor can demonstrate compliance with ISA-99 to some degree.

2
DEFINITIONS AND TERMINOLOGY

This section provides definitions, acronyms, and abbreviations for key terms as they are used in this report.

2.1 Definitions

Critical asset. A **digital** component of a critical system or infrastructure that, if compromised, represents a significant risk. A discussion of the definition of critical infrastructure and key assets can be found in Congressional Research Service (CRS) Report for Congress, *Critical Infrastructure and Key Assets: Definition and Identification* [4]. NERC-CIP-002-4, "Cyber Security – Critical Cyber Asset Identification: Attachment 1," specifically defines critical cyber assets for the U.S. electrical grid [5]. Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities, Appendix A, Section 3.1, Analyzing Digital Computer Systems," specifically defines the criteria for determining what is a critical digital asset for U.S. nuclear plants [6]. NEI 10-04, Revision 1, "Identifying Systems and Assets Subject to the Cyber Security Rule" provides guidance on determining nuclear critical digital assets [7].

In this report, *critical asset* is interpreted to mean critical digital assets, critical cyber assets, or critical assets that are defined in various ways according to the governing standard and the buyer's cybersecurity policies and procedures. This report **does not** provide guidance for how a critical asset is identified. The report assumes that the buyer has a method for identifying a critical asset, and the standard or guidance listed applies to identified critical assets.

Instrumentation and control (I&C) systems. Supervisory control and data acquisition (SCADA), process control system (PCS), distributed control system (DCS), and so on generally refer to the systems that control, monitor, and manage the nation's critical infrastructures such as electric power generators, subway systems, dams, telecommunication systems, and natural gas pipelines. Simply stated, a control system gathers information and then performs a function based on established parameters and/or information received.

Secure development and operational environment (SDOE). *Secure development environment* is defined as the condition of having appropriate physical, logical, and programmatic controls during the system development phases (that is, concepts, requirements, design, implementation, and testing) to ensure that unwanted, unneeded, and undocumented functionality (such as superfluous code) is not introduced into digital safety systems. *Secure operational environment* is defined as the condition of having appropriate physical, logical, and administrative controls in a facility to ensure that the reliable operation of digital safety systems is not degraded by undesirable behavior of connected systems and events initiated by inadvertent access to the system. RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," defines the requirements for an SDOE for nuclear safety systems [8].

System or software development life cycle (SDLC). Each organization is generally expected to have its own life cycle that is thoughtfully and purposefully created and followed to ensure high quality. Several standards and methodologies are available as references or for use, such as IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" [9], or ISO/IEC 12207:2008, "Systems and Software Engineering – Software Life Cycle Processes" [10].

Software development refers to a process used by a software developer to build application, basic, or firmware code. This process is commonly known as the software development life-cycle (SDLC) methodology and encompasses all activities to develop an application system and put it into production, including requirements gathering, analysis, design, construction, implementation, and maintenance stages. Examples of the SDLC methodology include, for example, waterfall, iterative, rapid, spiral, RAD, and Xtreme.

An SDLC is a well-defined, disciplined, and standard approach used in developing applications that provides the following:

- A methodical approach to solving business and information technology problems
- A method of managing, directing, monitoring, and controlling the process of application/software building, including:
  - A description of the process, that is, steps to be followed
  - Deliverables such as reports, programs, and documentation

Development assets and development environment. A *development asset* is defined as a digital device or system that is used for the development, testing, monitoring, or maintenance (in some cases, development assets are used for monitoring or maintenance in the operational environment for troubleshooting) of an I&C component or system in which the I&C component or system is intended for use as a critical asset by a utility. For example, consider a PC in a vendor's development environment that is used to configure the data in a controller that is being purchased by a utility. The controller will become a critical asset when installed on site and will be protected according to the utility's policies and procedures. However, the vendor's configuration PC is never installed on site but can be compromised by a cyber attack and therefore compromise the data on the controller prior to shipping; it is therefore a development asset that must be protected for nuclear safety systems and in other cases in accordance with the vendor's policies and procedures or as specified by the utility.

2.2 Acronyms and Abbreviations

AIS	automated information system
API	application program interface
ASA	adaptive security appliance
BTP	Branch Technical Position
C&A	certification and accreditation
CDA	critical digital asset
CGD	commercial grade dedication
CRP	coordinated research project
CRS	Congressional Research Service

CRT	communication robustness testing
CSMS	cybersecurity management system
CSPD	cybersecurity program description
DBT	design basis threat
DCS	distributed control system
DFAR	Defense Federal Acquisition Regulations
DHS	U.S. Department of Homeland Security
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DII	defense information infrastructure
DMZ	demilitarized zone
DOD	U.S. Department of Defense
DODI	DOD Instruction
DOE	U.S. Department of Energy
DOI	U.S. Department of the Interior
DOJ	U.S. Department of Justice
EDSA	embedded device security assurance
EPCIP	European Programme for Critical Infrastructure Protection
EPRI	Electric Power Research Institute
FAR	Federal Acquisition Regulation
FAT	factory acceptance test
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FSA	functional security assessment
I&C	instrumentation and control
IACS	industrial automation and control system
IAEA	International Atomic Energy Agency
ICS	industrial control system
IEC	International Electrotechnical Commission
IPS	intrusion prevention system
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISMS	information security management system
ISO	International Organization for Standardization
NASA	National Aeronautics and Space Administration
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NERC-CIP	NERC Critical Infrastructure Protection
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NITSL	Nuclear Information Technology Strategic Leadership
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
NSIR	U.S. Nuclear Security and Incident Response
NSSS	nuclear steam supply system

NUPIC	Nuclear Procurement Issues Committee
OMB	Office of Management and Budget
PCS	process control system
PFD	probability of failure on demand
PLC	programmable logic controller
QML	qualified manufacturers list
RFP	request for proposal
RG	Regulatory Guide
RRF	risk reduction factor
SAT	site acceptance test
SCADA	supervisory control and data acquisition
SDLC	software development life cycle
SDOE	secure development and operational environment
SDSA	software development security assessment
SIL	safety integrity level
SIS	safety instrumented system
SOW	statement of work
SP	Special Publication
SSEP	safety, security, and emergency preparedness
T&D	transmission and distribution
TS	top secret
VPN	virtual private network
WIB	Working-party on Instrument Behavior

3
BENCHMARK INTERVIEW RESULTS

This section consists of a compilation of the interview results for each question on the interview questionnaire. The results are summarized and represent the responses from the interviewees. Most of the comments are paraphrased and are not direct quotes. Many are a summary of a detailed verbal discussion in which the interviewee was asked whether the statement accurately represented their position. Most interviewees did not fill out the questionnaire. In the situations in which multiple interviewees made the same basic point, a single paraphrased comment was created. The basis for selection and paraphrasing of interviewee statements was 1) it had something to do with the question (vendors in particular often additional detail and insight beyond the question) and 2) many interviews tended to be long, detailed discussions, and it was expedient to paraphrase them into a condensed form.

This summary of the notes, with some analysis performed by the principal investigator, represents all of the comments from the interviewees. Each summary paraphrases and/or combines comparable interviewee responses, and the resulting analysis is in the cross-cutting themes and conclusions (see Section 4), even if they are the same statement. This benchmark effort set out to look for qualitative information in an effort to characterize available standards and good practices. It is not an exhaustive quantitative research effort.

For each question, the project team looked for **cross-cutting themes** that would be helpful for understanding the dominant requirements, practices, and thoughts in the field. Please note that cross-cutting themes are identified only by the principal investigator and the project team, not the interviewees, and they are based on a limited set of 16 interviews in a handful of industry sectors. A more widely cast net across more respondents in more industries might identify additional themes and insights or might simply confirm the themes identified here.

3.1 Interviewee Comments on Cybersecurity Standards and Guidance

Some interviewees had the following specific comments on standards and guidance, as described next.

3.1.1 Nuclear Sector

The following are specific comments from interviewees about nuclear sector standards and guidance:

- There are no clear standards or guidance on cybersecurity procurement specifications, nor are any standards or guidance consistently being used by nuclear plants. This lack of clarity and consistency results in ambiguity in the procurement of critical I&C systems. It appears that the plant personnel are struggling with what questions to ask. NEI 08-09 is the standard that many U.S. nuclear plants are attempting to use on a generic basis, and they will be adopting NEI 10-09 over time. NEI 10-09 Revision 0, "Addressing Cyber Security Controls for Nuclear Power Reactors, Section 11 (draft)" has some guidance on security of the supply chain [11].
- Many nuclear utilities are developing their own cybersecurity procurement guidance based on NEI 08-09 or are just listing the requirements of NEI 08-09 or RG 5.71, "Cyber Security Programs for Nuclear Facilities" [12], in their procurement specifications. Requirements are frequently "cut and paste" clauses that ask for more than is what required.
- Some utilities have no specific policies or procedures in place but are in some stage of development.
- Some utilities have developed a procurement procedure with a graded approach based in part on NEI 04-04, "Cyber Security Program for Power Reactors" [13], and NEI 08-09. Simple and complex examples are included with a series of questions are sent as part of a request for proposal (RFP).
- Some nuclear buyers are referencing NEI 08-09, Section E-11, "Cyber Security Plan for Nuclear Power Reactors" [1], on supply chain as a starting point for procurement requirements and/or guidance.

3.1.2 Other Sectors

The following are specific comments from interviewees about other sector standards and guidance:

- The federal government focuses on performance standards and specifications rather than design specifications to allow for innovation in proposed solutions.
- NERC-CIP is often used for Smart Grid critical infrastructure procurement.
- Some commercial and nonnuclear utilities are using DHS *Cyber Security Procurement Language for Control Systems* [14] and WIB Report M 2784 -X - 10, Revision 2, "Process Control Domain – Security Requirements for Vendors" [15], as a basis in procurement specifications, particularly in the chemical process industry.
- Some vendors prefer the DHS *Cyber Security Procurement Language for Control Systems* language. It has much detail but is not as prescriptive as WIB, which requires that certain activities be done by certain vendors (for example, accreditation or certification by Wurldtech or others). Many buyers put the DHS procurement language in their specifications, but they tailor it for their use. Dutch companies such as Shell use the WIB document (primarily because Shell is a Dutch organization).

- Some vendors are adopting certain standards such as ISA-99, ISASecure, or NERC-CIP to develop their systems.
- Some procurement specifications reference ISA-99.
- U.S. Department of Defense (DOD) procurements often require DOD Information Assurance Certification and Accreditation Process (DIACAP) accreditation for operational systems.

3.1.3 Cross-Cutting Themes

This section has yielded several overall cross-cutting themes that are described in Section 4, "Conclusions and Observations."

3.2 Standards and Guidance Documents in Use or Planned for Use

The following is a list of existing cybersecurity standards, guidance, and/or other guidance or standards projects that interviewees have indicated are used or are planned for use in the procurement of I&C critical assets. It is important to note that this is a list resulting only from the interviews and is not an exhaustive or complete list; this research project did not set out to systematically find all available cybersecurity guidance worldwide.

This list is organized by standards, standards guidance, and procurement guidance where possible.

A full citation (including hyperlinks to sources) and brief description of each document, and in some cases, how it is used, is provided in Appendix C.

3.2.1 Cybersecurity Standards and/or Standards Guidance

Interviewees indicated that they are using or are planning to use the following cybersecurity standards and/or standards guidance in the procurement of I&C critical assets:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations" [16].
- Federal Information Processing Standards (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems" [17], FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" [18], and NIST SP 800-53.
- FIPS 199, FIPS 200, and FIPS 140-2, "Security Requirements for Cryptographic Modules" [19].
- NIST SP 800-82 Final (June 2011), "Guide to Industrial Control Systems (ICS) Security" [20].
- NIST Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security, Volumes 1–3" [21]. This document includes cybersecurity requirements and risk analysis methods for the systems that will be implemented in the Smart Grid.
- NISTIR 7622, "Piloting Supply Chain Risk Management Practices for Federal Information Systems" [22].

- Office of Management and Budget (OMB) Circular No. A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities" [23].
- OMB Circular No. A-4, "Regulatory Analysis: The Presumption Against Economic Regulation" [24].
- OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources" [25].
- Federal Acquisition Regulation (FAR), a series of regulations [26]. In addition, there are also department acquisition regulations (U.S. Department of Justice [DOJ], U.S. Department of Energy [DOE], U.S. Department of the Interior [DOI], and DOD) and department/agency supplements (National Aeronautics and Space Administration [NASA], U.S. Air Force, DOD, and U.S. Army Corps of Engineers). The Defense Federal Acquisition Regulations (DFAR) is used by DOD and the intelligence agencies. The FAR and any associated supplements are mandatory for federal agencies.
- U.S. Nuclear Regulatory Commission (NRC) RG 5.71 [6].
- NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors" [1].
- NERC-CIP-002-009, "Cyber Security – Critical Cyber Asset Identification" [3].
- RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" [8].
- IEC 61226, "Nuclear Power Plants – Instrumentation and Control Important to Safety: Classification of Instrumentation and Control Functions" [27].
- IEC/TS 62443-1-1 Edition 1.0 (2009-07-30), "Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models" [28].
- IEC 62443-2-1 Edition 1.0 (2010-11-10), "Industrial Communication Networks – Network and System Security – Part 2-1: Establishing an Industrial Automation and Control System Security Program" [29].
- IEC/TR 62443-3-1 Edition 1.0 (2009-07-30), "Industrial Communication Networks – Network and System Security – Part 3-1: Security Technologies for Industrial Automation and Control Systems" [30].
- IEC 62443-2-4 Edition 1.0, "Security for Industrial Process Measurement and Control – Network and System Security – Part 2-4: Certification of IACS Supplier Security Policies and Practices," project targeted for 2012 release [31].
- ANSI/ISA-99, "Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program" [32].
- IEC 62645 Edition 1.0, "Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programmes for Computer-Based Systems," project targeted for 2012 release [33].
- International Atomic Energy Agency (IAEA), *International Atomic Energy Agency Reference Manual, Computer Security at Nuclear Facilities* [34].

- ISO/IEC 27000 Series:
  - ISO/IEC 27000, “Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary” [35].
  - ISO/IEC 27001, “Information Technology – Security Techniques – Information Security Management Systems – Requirements” [36].
  - ISO/IEC 27002, “Information Technology – Security Techniques – Code of Practice for Information Security Management” [37].
  - ISO/IEC 27003, “Information Technology – Security Techniques – Information Security Management System Implementation Guidance” [38].
  - ISO/IEC 27004, “Information Technology – Security Techniques – Information Security Management – Measurement” [39].
  - ISO/IEC 27005, “Information Technology – Security Techniques – Information Security Risk Management” [40].
  - ISO/IEC 27006, “Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems” [41].
  - ISO/IEC 27011, “Information Technology – Security Techniques – Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002” [42].
  - ISO/IEC 27031, “Information Technology – Security Techniques – Guidelines for Information and Communications Technology Readiness for Business Continuity” [43].
  - ISO/IEC 27033, “Information Technology – Security Techniques – Network Security – Part 1: Overview and Concepts and Part 2: Guidelines for the Design and Implementation of Network Security” [44].
  - ISO 27799, “Health Informatics – Information Security Management in Health Using ISO/IEC 27002” [45].
- ISO 28000, “Specification for Security Management Systems for the Supply Chain” [46].
- DOD DIACAP (new), DITSCAP (old), Department of Defense Information Assurance Certification and Accreditation Process
- EPRI report 1019187, *Technical Guideline for Cyber Security Requirements and Life Cycle Implementation Guidelines for Nuclear Plant Digital Systems* [47].
- EPRI report TR-106439, *Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications* [48].

3.2.2 Cybersecurity Guidance for Applying Standards

Interviewees indicated that they are using or are planning to use the following cybersecurity guidance for applying standards in the procurement of I&C critical assets:

- NEI 10-04, Revision 1, "Identifying Systems and Assets Subject to the Cyber Security Rule" [7].
- NEI 10-09 Revision 0, "Addressing Cyber Security Controls for Nuclear Power Reactors" (draft) [11].
- ISASecure (see Appendix C).
- IAEA Coordinated Research Project (CRP) on Cyber Security of Digital I&C Systems in Nuclear Power Plants. This is a project similar to EPRI and NEI efforts but does not appear to address procurement guidance; it does, however, contemplate developing best practices.
- European Commission, *A Reference Security Management Plan for Energy Infrastructure* [49].
- IEC EN 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems" [50].

3.2.3 Cybersecurity Procurement Guidance

Interviewees indicated that they are using or are planning to use the following cybersecurity procurement guidance in the procurement of I&C critical assets:

- WIB Report M 2784 X 10, Revision 2, "Process Control Domain – Security Requirements for Vendors" [15].
- DHS, *Cyber Security Procurement Language for Control Systems* [14].
- ISASecure (see Appendix C).
- IEC 62443-2-4, a proposed project to update IEC 62443 with IEC 62443-2-4 based on WIB for cybersecurity procurement guidance for general control systems.

3.2.4 Cross-Cutting Themes

The more interviews and research that were conducted, the more projects to address development of cybersecurity standards and guidance were discovered. At the time of publication, additional cybersecurity information sources, standards, and guidance were still being identified by interviewees and other interested participants from a variety of sectors. Over the course of Phase 1 of this project, the scope of the majority of the identified projects began to overlap on several major themes (for example, variations of NIST 800-53 requirements and WIB guidance).

3.3 Methods for Identifying Critical Assets

Interviewees indicated that they are using or are planning to use the following methods for identifying critical assets:

- In many cases, no method for identifying critical assets has been formally adopted by utilities or vendors.
- An internal risk assessment method is used in some cases.

- NEI 10-04, Revision 1, provides a method to identify critical digital assets (CDAs) for nuclear utilities [7].
- The federal government typically does not distinguish CDAs from other assets. The federal government selects cybersecurity **products** based on the impact if confidentiality, integrity, and/or availability of **IT assets** are compromised. For most IT systems, confidentiality and integrity are the most important security objectives. (For most control systems, availability and integrity are the most important security objectives.)
  - The levels of potential impact are low, moderate, and high for most unclassified systems. The impact level is selected based on the harm that could be done to an organization's assets, operations, or personnel (or to public welfare).
  - For classified systems, the level of potential impact is also based on the classification level of the system, for example, secret, top secret (TS), TS/sensitive compartmented information, and TS/compartmented. Critical assets are determined based on the impact level if the system is compromised.
  - In general, the federal government does not uniquely categorize critical assets. (Note: government **critical assets** could be those systems that have a high impact level for confidentiality and integrity or availability.)
- Some vendors design their systems to be protected as critical assets whether or not they are used as a critical asset by a buyer.
- IEC 61226, "Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions" is used by utilities in the United Kingdom as a standard for identifying critical assets.
- Some vendors differentiate by safety instrumented systems (SIS) and safety integrity levels (SIL) classification (based on petrochemical standards for SIS and SIL). On request, these vendors can and will build SIL 4 (highest level) and impose SDLC and cyber requirements. Vendors also look at critical—but non-safety—applications and still try to move up the SIL levels (SIL 3 for some critical applications).

3.3.1 Cross-Cutting Themes

A variety of methods with varying degrees of guidance is currently available for determining which assets are critical assets, based on the standard that is referenced by the interested organization.

3.4 Differentiation Between Safety-Related and Non-Safety-Related Critical Assets

Interviewees indicated that they are or plan to differentiate between safety-related and non-safety-related critical assets in the following ways:

- In many nonnuclear cases, no differentiation is made between safety-related and non-safety-related critical assets.

- In nuclear plants, safety-related systems and non-safety-related systems are differentiated according to the NRC definitions of those terms. There are different QA requirements for safety-related and non-safety-related systems. However, safety-related and non-safety-related CDAs are not differentiated in regard to cybersecurity requirements.
- Many federal departments and agencies have additional guidance documents for safety-related systems (for example, infrastructure and systems that are important for industrial safety and equipment protection).
- Some vendors tend to differentiate by SIL classification (based on petrochemical standards for SILs). On request, these vendors can and will build SIL 4 (highest level) and impose SDLC and cyber requirements. They also look at critical—but non-safety—applications and still try to move up the SIL levels (SIL 3 for some critical applications).
- In some nonnuclear cases, a risk assessment is performed to determine the safety protection level, and the results of the risk assessment are reflected in the procurement specification.

3.4.1 Cross-Cutting Themes

Nuclear CDAs are not differentiated between safety and non-safety and do not contemplate a graded approach based on risk.

For nonnuclear critical assets, varying methods are used in various sectors to assess the risk level of the asset and grade the cybersecurity requirements based on the potential risk to safety or critical operations.

3.5 Differentiation Between Technical and Programmatic Controls

Interviewees indicated that they are or plan to differentiate between technical and programmatic controls in the following ways:

- In many cases, no differentiation is made.
- In some cases, technical controls designated as the vendor's responsibility are differentiated from programmatic controls that are designated as the buyer's responsibility. Programmatic controls are typically the responsibility of the buyer.
- Technical controls are often derived by a programmatic control (derived in the sense that a programmatic control, such as a password change policy, requires a technical feature before it can be implemented). Some programmatic controls are difficult for a vendor to accomplish because they are more often a control that is assigned to the customer. Some are attempting to use ISA-99.03.03, "System Security Requirements and Security Assurance Levels" [51] and identify technical requirements that are derived from programmatic requirements (such as password changes).
- Each U.S. federal department, agency, and organization identifies the specific technical requirements for a system. These are included in the statement of work (SOW) for the project and are commonly included in a separate volume of the RFP. Programmatic requirements, such as managing the project and budgeting, are included in separate volumes of the RFP.

- In some cases, the application of each type of control is evaluated based on three basic distinctions:
  - Requirements during product development
  - Requirements during application development for a project
  - Requirements for support after a project

3.5.1 Cross-Cutting Themes

Programmatic controls are typically the responsibility of the buyer; however, many of the programmatic controls drive the technical controls and must be considered in the requirements.

3.6 Differentiation Between Integrators and Manufacturers

Interviewees indicated that they are or plan to differentiate between integrators and manufacturers in the following ways:

- Integrators typically fall under much greater scrutiny and have more complete and detailed requirements imposed on them.
- In the future, it is anticipated that utilities will require integrators to be responsible for the entire supply chain.
- In some nuclear utility cases, the focus of the supply chain cybersecurity program is on suppliers who handle CDAs, not those that handle the parts and components of CDAs. Therefore, concentration is on the system integrators and component manufacturers that handle finished CDAs.
- In some cases, no differentiation is made between integrators and equipment manufacturers.
- For U.S. federal procurement in general, the requirements are specific to the procurement and depend on the cybersecurity impact level for the system.
- The FAR specifies a qualified manufacturers' list (QML), a list of manufacturers that have had their products examined and tested and that have satisfied all applicable qualification requirements for that product.
- In some U.S. federal procurement cases, hardware and/or software components are excluded because of known vulnerabilities or country of origin. *Exclusion* in this context means "do not buy" and may be driven down to the subcomponent level (for example, certain processor types or chipsets).

3.6.1 Cross-Cutting Themes

Integrators are often held to a higher standard than a component manufacturer.

Integrators are likely to be held responsible for satisfying the requirements for all of the suppliers in the supply chain.

3.7 Supplier Development Environment

Interviewees indicated that they are or plan to consider the following aspects of the supplier development environment:

- The supplier development environment is often not considered in the procurement process.
- It is sometimes addressed in the nuclear sector for safety-related systems by referencing other documents such as RG 1.152, RG 5.71, Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" [52], and NEI 08-09. In addition, in many cases, the development environment only for nuclear safety-related systems is required to demonstrate cybersecurity compliance.
- Some buyers in the nuclear sector require that the supplier's development environment have an adequate cybersecurity program. It is not necessarily required for the supplier to conform to any one standard (for example, RG 5.71 or ISA-99) but will accept any cybersecurity program that can demonstrate protection of development assets and CDAs in the development environment.
- For U.S. federal procurement, as stated in the FAR, contracting officers shall:

  > (c) Request and consider the advice of specialists in audit, law, engineering, information security, transportation, and other fields, as appropriate.

  Each organization is required to perform a risk assessment for systems prior to developing the procurement specification. This risk assessment will assist the organization in selecting the appropriate baseline of cyber security controls from NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," May 2010.

- Most buyers tend to look more for a structured SDLC from suppliers than to impose cyber requirements on development assets per se.
- Some vendors are choosing to apply ISA-99, ISASecure, or other standards such as ISO 27000 series to certain development environments. In some of these cases, self-imposed adoption of a recognized cybersecurity standard allows the vendor to obtain an edge over competitors as cybersecurity expectations emerge from buyers in various sectors.

3.7.1 Cross-Cutting Themes

In most cases, the cybersecurity requirements for the vendor development environment are not addressed.

Many of the buyers and vendors believe that the vendor SDLC process that they have implemented for the development of critical assets satisfies the cybersecurity requirements for development assets.

The nuclear SDOE stipulated in RG 1.152 addresses only safety-related CDAs.

3.8 Requirements for Cybersecurity Testing Prior to Acceptance

Interviewees indicated that they are or plan to consider requirements for cybersecurity testing prior to acceptance:

- Custom requirements are sometimes included by the buyer.
- In many cases, no formal method for cybersecurity testing has been formally adopted. However, nearly all sectors have formal SDLCs in one form or another, and they all require some level of functional testing. Although there appears to be an absence of formal cybersecurity test methods, cybersecurity test cases are usually developed on a case-by-case basis by experienced and reputable practitioners who recognize the opportunity to run them in the test phase of their SDLC.
- With any cybersecurity, a large amount of testing is done before any live implementation of the system. Key areas that are tested include the following:
  - Functional behavior
  - Mechanical stability
  - Vulnerability (to common attacks)
  - System capabilities (as advertised)
- In some cases, cybersecurity testing is incorporated into factory acceptance test (FAT) and site acceptance test (SAT) (particularly when the DHS or WIB guidance is used), and post-modification tests using cybersecurity specialists. No formal cybersecurity procedure is in place.
- As stated in the FAR, Subpart 7.1 Acquisition Plans [53]:

  > (13) *Test and evaluation.* To the extent applicable, describe the test program of the contractor and the Government. Describe the test program for each major phase of a major system acquisition. If concurrency is planned, discuss the extent of testing to be accomplished before production release.

  The specific cybersecurity test requirements are defined by each organization for each system.
- Some vendors are using a Wurldtech testing box to test for communications robustness and vulnerabilities. However, it has limitations; it cannot, for example, test USB ports.
- Some nuclear utilities expect to adopt portions of NEI 10-09 [11] (in addition to NEI 08-09) in the future.

3.8.1 Cross-Cutting Themes

In cases in which the buyer uses ISA-99, DHS, or WIB, FAT and SAT requirements are typically addressed.

In the cases in which ISA-99, DHS, and WIB are not used, the buyer typically specifies generic testing requirements and relies on the vendor to demonstrate compliance using the vendor's SDLC.

Experienced and reputable vendors develop and apply cybersecurity test cases in their SDLC. However, there is no evidence that formal cybersecurity test methods or policies have been developed or adopted.

3.9 Requirements for Supply Chain Integrity

Interviewees indicated that they are or plan to consider requirements for supply chain integrity:

- Some buyers are currently developing a supply chain cybersecurity oversight program. This program will include cybersecurity audits, qualification of suppliers, inspections, and other oversight activities.
- Many requirements address only physical integrity.
- In some cases, supply chain integrity is ensured at the following three common points with any supplier:
  - Financial health of the supplier
  - Support agreements with the supplier
  - Research into any past public issues with the supplier in question
- NIST has published a draft NISTIR 7622, "Piloting Supply Chain Risk Management Practices for Federal Information Systems," that focuses on supply chain. In addition, U.S. federal agencies are specifying requirements in their procurement documents for the prime contractor and the subcontractors to ensure that supply chain integrity is maintained.
- In some cases, testing of the components or systems is used when received.
- Some vendors are self applying ISO 90001.
- Some nuclear utilities expect to adopt portions of NEI 10-09 in the future.

3.9.1 Cross-Cutting Themes

Several approaches are being evaluated and implemented in the area of supply chain integrity.

3.10 Actions and Compensating Controls When Vendor is Unable to Comply

Interviewees indicated that they are or plan to consider requirements for actions and compensating controls when a vendor is unable to comply:

- Although many buyers deal with vendors unable to fully comply with specified I&C cybersecurity requirements, they have not developed procedures or guidance at this point.
- In some cases, a vendor will be disqualified from further consideration if there are too many exceptions or the buyer cannot feasibly apply compensating controls.
- In other cases, if the vendor is already in place, a compensating control (for example, intrusion prevention system [IPS] to protect Cisco adaptive security appliances [ASAs]) is used until new equipment can be purchased and brought on-line.
- In many cases, a specific risk analysis is performed depending on how and where a component and/or system is used, along with a cost/benefit analysis, although these analyses are not formal. These analyses are coupled with specific testing.

- The NIST documents that address cybersecurity state when compensating controls must be implemented, but they do not provide guidance on what compensating controls are required or how to apply them. For control systems, NIST SP 800-53, Appendix I, "Recommended Security Controls for Federal Information Systems and Organizations," [16] interprets the security controls in the body of the SP.
- In most cases, buyers focus mostly on testing as an action to determine the controls that are in place and to determine the compensating controls that need to be applied. Third-party items are then integrated into systems using their structured SDLC. Sector-specific cyber requirements are dealt with on a project-by-project basis.
- For many buyers, some small hardware and/or software items from commercial shops that cannot or will not take any requirements must still be addressed. For example, sometimes drivers or application program interfaces (APIs) are required for certain functions. The API is downloaded from a website, then the API goes through extensive testing (see previous bulleted item) to ensure quality and security. The extent to which this testing is done depends on the end use application.

3.10.1 Cross-Cutting Themes

Many buyers will accept noncompliant I&C components and will perform a risk analysis and rigorous testing using their own SDLC in order to accept the component.

There is no clear standard or guidance on how to accept a noncompliant I&C vendor or component or how to evaluate an I&C vendor for compliance with cybersecurity requirements.

3.11 Are Security and Other Systems Allowed to Store Data in the "Cloud"?

Interviewees indicated that they are or plan to consider requirements regarding whether security and other systems are to be allowed to store data in the cloud:

- For CDAs in nuclear plants, data are not allowed to be stored in the cloud.
- NRC contradictions sometimes cause issues with both system design and operation: rigid change controls from I&C branch contrasted with need for frequent patching and upgrading by U.S. Nuclear Security and Incident Response (NSIR) branch (to deal with new vulnerabilities) with no cloud computing or connectivity allowed.
- In some cases outside the nuclear sector, absolutely no security tools are used that either function or store information in the cloud.
- In other cases, the response is specific to each system. The use of cloud technology is encouraged in the U.S. federal government.
- Some vendors report that cloud-based services are not allowed by some buyers but are allowed by others.
- Some vendors have included the cloud as a key strategy for their business, and the use of the cloud is growing.
- In a few cases, cloud services are not allowed, but interviewees are examining this question. Customers who want connectivity for vendor support are still using enterprise-based edge connections, and then only for data historian functions so that the vendor can help correct problems.

3.11.1 Cross-Cutting Themes

Buyers vary on allowing the use of the cloud with no clear trend identified.

Nuclear CDAs are not allowed to store data in the cloud.

NRC policy contradictions are causing issues for utilities and vendors. Outside the nuclear sector, the use of software, services, and data storage in the cloud is growing rapidly, and many vendors are adopting the cloud in their strategy.

3.12 Where and How Remote Connectivity Is Allowed

Interviewees indicated that they are or plan to consider requirements regarding where and how remote connectivity is allowed:

- Two-way remote communication is not allowed in Level 4 or Level 3 protection levels in nuclear plants for CDAs, and may not be allowed in Level 2 or Level 1 depending on the utility's cybersecurity program policies and procedures.
- Remote access for maintenance is often performed through a shared, encrypted virtual private network (VPN) connection such as a cluster of Juniper SA 4500 SSL VPN systems. Access to the systems is typically monitored during maintenance by a member of the InfoSec team.
- Any general monitoring of security systems is usually performed by internal monitors under the control of the internal InfoSec team.
- For U.S. federal systems, remote access for monitoring and maintenance is acceptable. NIST has published some SPs that provide guidance for remote access. Most of the SPs focus on IT systems, not control systems.
- Most vendors support remote connectivity for their customers. They formerly used call-back modems and now use peripheral connections through demilitarized zone (DMZ) with latest VPN and security approaches. Aftermarket support is essential for patches and upgrades. Nuclear vendors are aware of NRC contradictions: rigid change controls from I&C branch contrasted with the need for frequent patching and upgrading by NSIR branch (to deal with new vulnerabilities).
- For some buyers and vendors, remote connectivity and monitoring is a requirement, such as in monitoring the activities of off-shore oil and gas mobile equipment. In these cases, a robust cybersecurity program is implemented.

3.12.1 Cross-Cutting Themes

NRC contradictions cause issues with both I&C system design and operation: dogmatic, rigid change controls from I&C branch contrasted with the need for frequent patching and upgrading by NSIR branch (to deal with new vulnerabilities) with no remote connectivity allowed.

Two-way remote communication is not allowed in Level 4 or Level 3 protection levels in nuclear plants for CDAs, and may not be allowed in Level 2 or Level 1 depending on the utility's cybersecurity program policies and procedures.

Remote connectivity is an accepted method used by many organizations, and it is supported by most vendors. Nuclear plants and some other organizations do not allow remote connectivity to critical assets based on regulation or internal policies and procedures.

3.13 Interviewee Recommendations

During the course of the interviews, interviewees made recommendations about how their industry and/or EPRI should proceed. Some interviewees volunteered recommendations in the context of their own industry, while others provided recommendations meant to be applied across multiple sectors. These points are **not** necessarily the recommendations from this project. A compilation and summary of recommendations are listed next.

3.13.1 Nuclear Sector

Interviewees made recommendations about how their industry and/or EPRI should proceed regarding the nuclear sector:

- Develop awareness and training for the procurement organizations. There is a significant gap between the wisdom and knowledge of the Nuclear Information Technology Strategic Leadership (NITSL) community and the procurement departments of the various plants.
- Recommend the high-level approach set forth here in developing cybersecurity procurement guidance. Procurement agents might not have the knowledge on how to apply controls effectively and, therefore, might not know specifically what (from NEI 08-09) to ask a vendor to do for their product. Specifying and classifying which controls should be used for which systems will improve the quality and clarity of the customer requirements.
    1. Simplify guidance so that plant procurement staff can effectively use it by creating "classes" of nuclear plant components with the same characteristics such as controllers, instruments, networks, computers, logging, and archiving.
    2. Then determine the appropriate group of controls to be expected for each class.
    3. Then provide an approach to grade by level and class. Each plant can augment where existing controls are already in place so that the vendor/supplier can better understand what is required by design and what can be leveraged and integrated into.
- NEI and EPRI should reach out to NSIR (and/or other NRC branches) and involve them in this process from the beginning.
- The industry should develop a cybersecurity program description (CSPD) template for NSSS suppliers, balance of plant system suppliers, system integrators, and other organizations involved in the supply chain for the commercial nuclear power industry. Current cybersecurity guidance applies to nuclear power plant licensees or to organizations of a kind much different than nuclear suppliers.
- Develop a cybersecurity audit capability similar to Nuclear Procurement Issues Committee (NUPIC) audits for the industry.

- Continuous monitoring from a service system or tool is a solid approach and appropriate for cybersecurity. The NRC is requiring a disconnect of these systems during normal operations that is causing a serious loss of capability (dumb down). EPRI should work with the NRC and others to explore methods for continuous monitoring to take advantage of operational and cybersecurity benefits that are available.
- The NRC has purchased systems from AREVA, Invensys, and Westinghouse, and it is testing for cybersecurity vulnerabilities in Sandia to understand attack vectors. EPRI should obtain information about the project and become involved in an appropriate manner.
- The process of commercial grade dedication (CGD) involves identifying the safety functions and associated critical characteristics of commercial components intended for safety-related use. Cybersecurity features are not part of the design basis safety function for these components; therefore, critical characteristics of a component do not and should not involve cybersecurity controls and/or features.
- The plant safety analysis considers control system malfunctions and single failures in safety systems concurrent with design basis events. System failure analysis is a necessary part of demonstrating its ability to withstand these postulated scenarios with **reasonable** assurance. However, design basis threats are not considered or postulated in the safety analysis. Instead, design basis threats, including cyber attacks, are postulated outside the safety analysis, where physical security and cybersecurity requirements and plans provide **high** assurance of protection against these threats and attacks. Therefore, failure analysis of control or protection systems should not postulate failures due to cyber attacks or failures of cybersecurity controls or features to mitigate such attacks.

3.13.2 Other Sectors

Interviewees made recommendations about how their industry and/or EPRI should proceed regarding other sectors:

- Coordinate with the IEC 62443-2-4 (proposed), IEC 62645, IAEA CRP, and NEI teams in developing cybersecurity procurement guidance for application to at least nuclear plants with consideration for nonnuclear generation and transmission and distribution (T&D); all adapted from WIB and DHS cybersecurity procurement guidance, using the language or approach from each where appropriate. The IEC 62443-2-4 project may provide sufficient guidance for T&D and nonnuclear generation.
- Understand and provide guidance on the role of penetration and other testing performed by specific vendors and/or devices.
- More integrated procurement specification of requiring everything on each asset is needed. No individual components are designed to take into account the appropriate integrated system controls such as logging and network monitoring.
- There are too many standards and guidance documents. The industry needs to consolidate them into a set of standards and guidance that are accepted by all.

3.13.3 Cross-Cutting Themes

Development of consistent guidance that can be accepted by all parties is needed.

DHS and WIB are good benchmarks to use in developing more complete guidance and methods.

The guidance should include a method or template to simplify the application of cybersecurity controls.

Coordination with other standards bodies should be integrated.

4
CONCLUSIONS AND OBSERVATIONS

The conclusions presented in this section are based on the collective significance of interview responses as judged by the principal investigator and by the EPRI Technical Advisory Committee. The benchmark did not set out to acquire any measurable data other than a simple Q&A method for inducing responses in an effort to characterize available standards and good practices in a qualitative manner. The observations are based on the principal investigator's overall impressions from the interviews, which were frequently lengthy conversations that covered several areas not necessarily directly related to the interview question.

Some of the conclusions and observations overlap with some of the comments and cross-cutting themes from Section 3. Because the comments and cross-cutting themes are a paraphrased summary and may also be interviewee conclusions or observations, they may also be applicable in this section.

4.1 Conclusions

The following are the conclusions of the interview responses:

- Almost every regulatory agency, governmental agency, standards body, and industry group has developed, is developing, or is proposing cybersecurity standards, guidance, and best practices.
- It appears that only WIB, DHS, and ISASecure have specific guidance related to cybersecurity procurement of I&C critical assets at the time of this report. WIB, ISASecure, and DHS are generic control system guidance with some references to Smart Grid critical infrastructure.
- Nuclear utilities have not developed a consistent method for applying cybersecurity standards to I&C vendors in the procurement process.
- Some nonnuclear utilities and commercial buyers are attempting to adopt the DHS, WIB, and in some cases, ISASecure guidance, as a cybersecurity procurement standard to be adapted on a project basis.
- Some control system vendors have self imposed a particular standard or guidance to demonstrate compliance, and some have taken the extra step to obtain a particular certification such as ISASecure.
- Most standards and guidance address, to some degree, protection of the supply chain.
- Most standards and guidance do not address vendor development assets and development environment other than limited configuration management, supply chain, and testing of cybersecurity features. Software development and configuration standards only partially address cybersecurity of the development assets themselves.
- Almost all interviewees expressed a desire for a common set of cybersecurity procurement best practices and guidance, with the exception of DOD vendors who believe that the DOD has applied a common set of practices.

4.2 Observations

The observations listed next are not direct conclusions from the benchmark study; rather, they are considered opinions of the project team after completing Phase 1 of this project:

- DHS and WIB contain useful cybersecurity procurement language and approaches. However, a significant gap exists between these documents and NEI 08-09 and RG 5.71. This is because of the unique requirements for U.S. nuclear and proposed standards for international nuclear plants. The gap can be characterized as follows:
  - The level of prescriptive detail with respect to topics such as defense-in-depth and security controls is much higher in nuclear-specific guidance documents than those guidance documents, such as DHS and WIB, used in other sectors.
  - On the other hand, general guidance documents such as DHS and WIB provide more guidance than nuclear-specific guidance on other topics such as remote access.
- Many buyers and vendors are confused by the number and variety of standards. Although the standards are not necessarily in conflict, they are often inconsistent and address varying aspects of the overall problem.
- Several projects are under way at NEI, IAEA, IEC, and others that will overlap with any future phases of this project. It might be desirable to spend the time to coordinate with their efforts in an attempt to reduce the confusion over standards and guidance for digital I&C cybersecurity.

5
PHASE 2 AND PHASE 3 RECOMMENDATIONS

Based on the results of Phase 1, the project team developed recommendations, currently under consideration by EPRI, for the proposed scope of Phases 2 and 3 of this project. EPRI reports 1019187, *Technical Guideline for Cyber Security Requirements and Life Cycle Implementation Guidelines for Nuclear Plant Digital Systems* [47], and TR-106439, *Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications* [48] were reviewed to determine whether there were methodologies or approaches that could be applied in Phases 2 and 3.

5.1 Considerations

In addition to the conclusions and observations described in Section 4, the following items were considered in recommending the scope of Phases 2 and 3 of this project:

- Vendors and their systems and components vary widely in how they have applied cybersecurity controls, from best case to worst case (think of them as ranked "groups" or "categories") such as:
  1. Fully nuclear NEI 08-09 compliant and auditable
  2. Have certified to some standard such as ISASecure
  3. Claim compliance with a cybersecurity standard (for example, NERC-CIP)
  4. Minimal cybersecurity controls, but some documentation
  5. Noncompliant although some controls are likely present
  – In many cases, procuring critical assets will require a risk assessment and cost/benefit analysis for acceptance based on degree of testing and compensating controls required.
- Many controls do not apply in many cases:
  – They depend on the intended use in the plant and subsequent data flow.
  – They depend on the type of component.
  – Similar data flows (and associated use cases) and similar components will have a known subset of controls that are required and might usually be in place.
- Copying cybersecurity requirements from any given standard and pasting them into a procurement specification does not really work.
- DHS and WIB categorize some types of systems and use cases to some degree, with useful language, but they do not address all of these considerations.

5.1.1 Final Conclusion

It is appropriate for EPRI to move forward with Phases 2 and 3 of this project, as described next.

5.2 Recommendations for Phase 2 – Cybersecurity Procurement Methodology and High-Level Specifications

The project team recommends that a procurement methodology be developed in Phase 2, along with initial high-level specifications, in order to create a practical and consistent approach prior to developing detailed specifications and guidance (Phase 3). The scope of Phase 2 includes the following tasks:

1. Develop a generic method for identifying cybersecurity requirements and controls based on typical use case and data flow of the procured component or system. The goal is to create categories based on data flows, components, or systems that have similar reusable requirements. These categories will be clearly described and will include some high-level specification language and guidance for each category.
2. Develop a generic method for identifying vendor cybersecurity capabilities based on expected vendor compliance, with the understanding—based on benchmark results from Phase 1—that vendors are compliant in varying degrees with various standards. It is assumed that vendors with similar capabilities can be grouped together to allow buyers to know what to expect from each group. The generic method for identifying vendor cybersecurity capabilities will be clearly described and will include some high-level specification language and guidance.
3. Develop a generic approach for performing qualitative risk assessments, cost/benefit analyses, and the application of compensating controls for those cases in which a procured component or system does not meet the full set of requirements. This approach is **not** a formal engineering or licensing procedure or analysis. It is intended as a practical approach for the I&C engineer, cybersecurity specialist, and procurement officer (or purchasing agent) to work together to evaluate the implications of purchasing a component that does not meet the full set of requirements. That is, such risk assessments and cost/benefit analyses are expected to be more qualitative in nature than quantitative.
4. The guidance and methods from Tasks 1, 2, and 3 are intended for use across the electric utility industry where possible. Any nuclear-specific language or approaches will be clearly identified.
5. An EPRI technical update report that includes this information will be published.

5.3 Recommendations for Phase 3 – Detailed Cybersecurity Specification Language and Guidance Documents

The project team recommends that more detailed guidance, procedures, and worked examples be developed in Phase 3 based on the methods that were developed in Phase 2. The scope of Phase 3 includes the following tasks:

1. Develop more detailed guidance and worked examples for the methods developed in Phase 2.
2. Develop generic cybersecurity procurement specification language based on the methods developed in Phase 2.
3. Develop a procedure template for implementing the methods developed in Phase 2.
4. The methods, specifications, guidance, examples, and procedure template will reference and use existing standards and guidance where possible, intended for use across the electric utility industry (again, where possible). Any nuclear-specific language or approaches will be clearly identified.
5. An EPRI technical update report that includes this information will be published.

6
REFERENCES

1. NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors.” Nuclear Energy Institute, Washington, DC. 2009.
2. ISA-99, “Industrial Automation and Control Systems Security.” International Society of Automation, Research Triangle Park, NC.
3. NERC-CIP-002-009, “Cyber Security – Critical Cyber Asset Identification.” North American Electric Reliability Corporation, Princeton, NJ.
4. CRS Report for Congress, *Critical Infrastructure and Key Assets: Definition and Identification.* (Order Code RL 32631) Congressional Research Service, Library of Congress, Washington, DC. 2004.
5. NERC-CIP-002-4, “Cyber Security – Critical Cyber Asset Identification: Attachment 1, Critical Asset Criteria.” North American Electric Reliability Corporation, Princeton, NJ.
6. Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities, Appendix A, Section 3.1, Analyzing Digital Computer Systems.” Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission.
7. NEI 10-04, Revision 1, “Identifying Systems and Assets Subject to the Cyber Security Rule.” Nuclear Energy Institute, Washington, DC.
8. Regulatory Guide 1.152, Revision 3. “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.” Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission.
9. IEEE Standard 1074-1995. “IEEE Standard for Developing Software Life Cycle Processes.” IEEE, New York, NY. 1995.
10. ISO/IEC 12207:2008, “Systems and Software Engineering – Software Life Cycle Processes.” International Electrotechnical Commission. 2008.
11. NEI 10-09 Revision 0, “Addressing Cyber Security Controls for Nuclear Power Reactors, Section 11” (draft). http://www.nei.org/.
12. Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities.” Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission.
13. NEI 04-04, “Cyber Security Program for Power Reactors.” Nuclear Energy Institute, Washington, DC. 2005.
14. Department of Homeland Security, *Cyber Security Procurement Language for Control Systems.* Control Systems Security Program, National Cyber Security Division. Washington, DC. 2009. http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf
15. “Process Control Domain – Security Requirements for Vendors.” Report M 2784 -X - 10, Revision 2. Working-party on Instrument Behavior, The Hague, The Netherlands. 2010.
16. NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations.” National Institute of Standards and Technology, Gaithersburg, MD. 2009.

17. FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems.” Federal Information Processing Standards, National Institute of Standards and Technology, Gaithersburg, MD. 2006.
18. FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems.” Federal Information Processing Standards, National Institute of Standards and Technology, Gaithersburg, MD. 2004.
19. FIPS 140-2, “Security Requirements for Cryptographic Modules.” Federal Information Processing Standards, National Institute of Standards and Technology, Gaithersburg, MD. 2002.
20. NIST Special Publication 800-82, “Guide to Industrial Control Systems (ICS) Security.” National Institute of Standards and Technology, Gaithersburg, MD. 2011.
21. NISTIR 7628, “Guidelines for Smart Grid Cyber Security, Volumes 1–3.” National Institute of Standards and Technology, Gaithersburg, MD. 2010.
22. NISTIR 7622, “Piloting Supply Chain Risk Management Practices for Federal Information Systems.” National Institute of Standards and Technology, Gaithersburg, MD. 2010.
23. OMB Circular No. A-119, “Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.” Office of Management and Budget, Washington, DC. 1998. http://www.whitehouse.gov/omb/circulars_a119_a119fr
24. OMB Circular No. A-4, “Regulatory Analysis: The Presumption Against Economic Regulation.” Office of Management and Budget, Washington, DC. 2004. http://www.whitehouse.gov/omb/circulars_a004_a-4/
25. OMB Circular No. A-130, Appendix III. “Security of Federal Automated Information Resources.” Office of Management and Budget, Washington, DC. http://www.whitehouse.gov/omb/circulars_a130_a130trans4/
26. Federal Acquisition Regulation (FAR). https://www.acquisition.gov/far/.
27. IEC 61226, “Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions.” International Electrotechnical Commission. 2009.
28. IEC/TS 62443-1-1 Edition 1.0 (2009-07-30), “Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models.” International Electrotechnical Commission. 2009.
29. IEC 62443-2-1 Edition 1.0, “Industrial Communication Networks – Network and System Security – Part 2-1: Establishing an Industrial Automation and Control System Security Program.” International Electrotechnical Commission. 2010.
30. IEC/TR 62443-3-1 Edition 1.0, “Industrial Communication Networks – Network and System Security – Part 3-1: Security Technologies for Industrial Automation and Control Systems.” International Electrotechnical Commission.
31. IEC 62443-2-4 Edition 1.0, “Security for Industrial Process Measurement and Control – Network and System Security – Part 2-4: Certification of IACS Supplier Security Policies and Practices.” (project targeted for 2012 release) International Electrotechnical Commission.

32. ANSI/ISA-99, “Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.” International Society of Automation, Research Triangle Park, NC. 2009. http://www.isa.org/standards.
33. IEC 62645 Edition 1.0, “Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programmes for Computer-Based Systems” (project targeted for 2012 release). International Electrotechnical Commission.
34. *International Atomic Energy Agency Reference Manual, Computer Security at Nuclear Facilities.* International Atomic Energy Agency, Vienna 2010.
35. ISO/IEC 27000, “Information Technology – Security Techniques – Information Security Management – Overview and Vocabulary.” International Organization for Standardization and International Electrotechnical Commission.
36. ISO/IEC 27001, “Information Technology – Security Techniques – Information Security Management Systems – Requirements.” International Organization for Standardization and International Electrotechnical Commission.
37. ISO/IEC 27002, “Information Technology – Security Techniques – Code of Practice for Information Security Management.” International Organization for Standardization and International Electrotechnical Commission.
38. ISO/IEC 27003, “Information Technology – Security Techniques – Information Security Management System Implementation Guidance.” International Organization for Standardization and International Electrotechnical Commission.
39. ISO/IEC 27004, “Information Technology – Security Techniques – Information Security Management – Measurement.” International Organization for Standardization and International Electrotechnical Commission. 2009.
40. ISO/IEC 27005, “Information Technology – Security Techniques – Information Security Risk Management.” International Organization for Standardization and International Electrotechnical Commission. 2011.
41. ISO/IEC 27006, “Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.” International Organization for Standardization and International Electrotechnical Commission. 2007.
42. ISO/IEC 27011, “Information Technology – Security Techniques – Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002.” International Organization for Standardization and International Electrotechnical Commission. 2008.
43. ISO/IEC 27031, “Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity.” International Organization for Standardization and International Electrotechnical Commission. 2011.
44. ISO/IEC 27033, “Information Technology – Security Techniques – Network Security – Part 1: Overview and Concepts and Part 2: Guidelines for the Design and Implementation of Network Security. International Organization for Standardization and International Electrotechnical Commission. 2009.
45. ISO 27799, “Health Informatics – Information Security Management in Health Using ISO/IEC 27002.” International Organization for Standardization. 2008.

46. ISO 28000, “Specification for Security Management Systems for the Supply Chain.” International Organization for Standardization. 2007.
47. *Technical Guideline for Cyber Security Requirements and Life Cycle Implementation Guidelines for Nuclear Plant Digital Systems.* EPRI, Palo Alto, CA: 2010. 1019187.
48. *Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications.* EPRI, Palo Alto: 2006. TR-106439.
49. Harnser Group, *A Reference Security Management Plan for Energy Infrastructure.* Prepared for the European Commission by the Harsner Risk Group Ltd. 2010. http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf.
50. IEC EN 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.” International Electrotechnical Commission.
51. ISA-99.03.03, “System Security Requirements and Security Assurance Levels.” International Society of Automation, Research Triangle Park, NC.
52. Branch Technical Position 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.” U.S. Nuclear Regulatory Commission. http://pbadupws.nrc.gov/docs/ML0706/ML070670183.pdf.
53. FAR, Subpart 7.1 Acquisition Plans https://www.acquisition.gov/far/current/html/Subpart%207_1.html.
54. 10 CFR 73.54, “Physical Protection of Plants and Materials: Protection of Digital Computer and Communication Systems and Networks.” Code of Federal Regulations. U.S. Nuclear Regulatory Commission.
55. Department of Defense Instruction 8510.01, “Department of Defense Information Assurance Certification and Accreditation Process (DOD DIACAP).” Washington, DC. 2007.
56. Department of Defense, “DIACAP Application Manual.” Washington, DC.

A
BENCHMARK QUESTIONNAIRE

Phase 1 – Procurement Requirements Benchmark

The overall project objective is to develop generic digital systems procurement cybersecurity requirements and specific procurement language with worked examples, along with guidance that utilities can use to procure digital equipment and systems and reduce the risk of costly rework after a system is implemented. The stated goal for the entire project is to assist utilities in preventing costly backfit to new digital equipment in order to meet cybersecurity commitments.

The purpose of Phase 1 is to perform a limited set of interviews with a cross section of various entities including nuclear, power generation, transmission and distribution, instrumentation and control (I&C) vendors, and others in order to capture existing procurement practices for digital systems. A benchmark study will be created based on the results of the interviews to determine whether existing standards and practices are in use that the Electric Power Research Institute (EPRI) can recommend or whether additional work is required to develop guidance for procurement of cybersecurity systems. If additional work is required, EPRI will use existing best practices to inform its work.

Questionnaire

The following questionnaire is to be used by an interviewer or to be filled out by an interviewee.

Confidentiality: The questionnaire results, the identity of the entity, and the identity of the individual interviewed will remain confidential and will not be published. The questionnaire results will be summarized in a benchmark study that will be published as an EPRI technical update. Only the industry and role of those interviewed will be identified.

Who do we wish to interview? For the best cross section of results, we wish to interview individuals from two different roles: 1) the individual with cybersecurity responsibility who is or has been involved with the specification and procurement of digital systems and 2) the individual in procurement/contracts who is responsible for creating the cybersecurity procurement language and procuring digital systems that require cybersecurity controls.

Table A-1
Questionnaire: Confidential Identification Information

Interviewer Name (if Applicable)	Name: Date Completed:
Interviewee Name and Contact Information	Name: Organization: Position/Role: Phone Number: E-mail Address:

Table A-2
Questionnaire

Question (Note: All questions are in the context of cybersecurity digital system procurement.)	Result
What cybersecurity standards are currently utilized to procure critical digital assets, if any? How and to what degree are they applied?	
Is there an existing cybersecurity procurement guidance document that is used? If so, to what extent?	
How are critical assets identified?	
Does your organization differentiate between safety-related and non-safety-related systems? If so, how are safety-related and non-safety-related digital systems treated differently; the same?	
How are technical versus programmatic requirements treated?	
Are integrators treated differently than manufacturers? If so, how?	
To what degree is the supplier development environment required to demonstrate cybersecurity compliance? What process or guidance was used to determine the extent?	

Table A-2 (continued)
Questionnaire

Question (Note: All questions are in the context of cybersecurity digital system procurement.)	Result
What cybersecurity testing is required prior to delivery and acceptance?	
How is supply chain integrity ensured?	
What actions and/or compensating controls are taken for required components when vendors are unable or unwilling to comply with cybersecurity requirements?	
For vendor I&C systems or security tools, do you allow the system to connect to or store data in the cloud? Are any of the vendor's security tools cloud based?	
Do you allow remote access for monitoring and maintenance? If so, what standards or guidance do you use for controls?	
Will you allow EPRI to acknowledge your company and your name in the project and any report deliverable?	
Additional notes.	

B
LIST OF INDUSTRIES AND CONTRIBUTORS

Of the contributors listed in the Acknowledgements Section, the following are those individuals and companies (in alphabetical order) that have contributed to the project and have also agreed to allow the project to list their names and organizations. EPRI would like to thank all contributors for their time, insights, and contributions to the project.

Name: Steve Batson, CISSP
Organization: Invensys Critical Infrastructure & Security Practice
Position/Role: Principal Consultant, Nuclear Cyber Security

Name: James P. Batug
Organization: PPL Generation, LLC
Position/Role: Engineering Support Manager- CIP

Name: Matthew Bohne
Organization: GE-Hitachi nuclear Energy (GEH)
Position/Role: Senior Engineer Advanced Plant Cyber Security and Networks

Name: Vic Fregonese
Organization: AREVA
Position/Role: Projects Director, I&C Electrical Systems

Name: William Gross
Organization: NEI
Position/Role: Project Manager, Security

Name: Curt Jensen
Organization: DN2K
Position/Role: CEO

Name: Annabelle Lee
Organization: EPRI
Position/Role: Technical Executive – Cyber Security

Name: Ted Quinn
Organization: Technology Resources
Position/Role: Principal, ANS Past President, IEC SC45A WGA9 Convener

Name: Ernie Rakaczky
Organization: Invensys Operations Management (IOM)
Position/Role: IOM Portfolio Manager

Name: Pat Samples, Ph.D.
Organization: Mitsubishi Nuclear Energy Systems, Inc.
Position/Role: Engineer, I&C and Electrical Engineering

Name: Jim Shank
Organization: PSE&G, Salem/Hope Creek
Position/Role: IT Manager

Name: Graham Speake
Organization: Yokogawa
Position/Role: Principal Systems Architect

Name: Kevin Staggs
Organization: Honeywell
Position/Role: Cyber Security Researcher

Name: Chris Sterba
Organization: Omaha Public Power District, Fort Calhoun
Position/Role: Supervisor Digital Design, nuclear Energy Division

C
CYBERSECURITY STANDARDS AND GUIDANCE

This section contains a list of existing cybersecurity standards, guidance, and/or other guidance or standards projects that interviewees have indicated are used or are planned for use in the procurement of I&C critical assets. It is important to note that this is a list resulting only from the interviews and is not an exhaustive or complete list; this research project did not set out to systematically find all available cybersecurity guidance worldwide.

C.1 Cybersecurity Standards and/or Standards Guidance

Interviewees indicated that they are using or are planning to use the following cybersecurity standards and/or standards guidance in the procurement of I&C critical assets:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," [16] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

  Although NIST SP 800-53 was developed as a U.S. federal standard, industry has adopted the principals and language in developing other cybersecurity standards. Although not strictly the "parent" of other standards, it serves as single requirements benchmark.

  It has been implemented in combination with Federal Information Processing Standards (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems," [17] and FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" [18].
- FIPS 200, FIPS 199, and NIST SP 800-53.

  FIPS 200 is a mandatory federal standard developed by NIST in response to the Federal Information Security Management Act (FISMA). To comply with the federal standard, organizations must first determine the security category of their information system in accordance with FIPS 199, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST SP 800-53. Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in SP 800-53, which allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation.
- FIPS 199, FIPS 200, and FIPS 140-2, "Security Requirements for Cryptographic Modules" [19] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

  See previous comments.

- NIST SP 800-82 Final (June 2011), "Guide to Industrial Control Systems (ICS) Security" [20] http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

  Finalized in June 2011, only one interviewee referenced the document; however, the content is specific and relevant. Although not a procurement guidance document, it might be a reasonable reference for the next phases of the project.

  This document provides guidance for establishing secure industrial control systems (ICSs). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other control system configurations such as skid-mounted programmable logic controllers (PLCs) are frequently found in the industrial control sectors. ICSs are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (such as automotive, aerospace, and durable goods). SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control. DCSs are generally used to control production systems in a local area such as a factory using supervisory and regulatory control. PLCs are generally used for discrete control for specific applications and generally provide regulatory control. These control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 90% of the nation's critical infrastructures are privately owned and operated. Federal agencies also operate many of the ICS mentioned previously; other examples include air traffic control and materials handling (for example, postal service mail handling.) This document provides an overview of these ICSs and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.
- NIST Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security, Volumes 1–3" [21]. Includes cybersecurity requirements and risk analysis methods for the systems that will be implemented in the Smart Grid. http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf.

  The three volume report, NISTIR 7628, presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of Smart-Grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of Smart Grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information presented in the report as guidance for assessing risk, and they can then identify and apply appropriate security requirements to mitigate that risk. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

- NISTIR 7622, “Piloting Supply Chain Risk Management Practices for Federal Information Systems” [22] http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf.

  This document was referenced by only one interviewee and might serve as a reference document for any supply chain guidance that is developed in the next phases.

  Draft NISTIR 7622, “Piloting Supply Chain Risk Management Practices for Federal Information Systems,” is intended to provide a wide array of practices that when implemented will help mitigate supply chain risk. It is this project’s intent that organizations begin to pilot the activities and practices in this report and provide feedback on the practicality, feasibility, cost, challenges, and successes. This is the first step in a much larger initiative of developing a comprehensive approach to managing supply chain risks that focuses on supply chain. In addition, federal agencies are specifying requirements in their procurement documents for the prime contractor and the subcontractors to ensure that supply chain integrity is maintained.
- As stated in Office of Management and Budget (OMB) Circular No. A-119, “Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities” [23]:

  > All federal agencies must use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical. In these circumstances, your agency must submit a report describing the reason(s) for its use of government-unique standards in lieu of voluntary consensus standards to the Office of Management and Budget (OMB) through the National Institute of Standards and Technology (NIST).
  >
  > For purposes of this policy, “voluntary consensus standards” are standards developed or adopted by voluntary consensus standards bodies, both domestic and international. These standards include provisions requiring that owners of relevant intellectual property have agreed to make that intellectual property available on a non-discriminatory, royalty-free or reasonable royalty basis to all interested parties. For purposes of this Circular, "technical standards that are developed or adopted by voluntary consensus standard bodies" is an equivalent term.

- OMB Circular No. A-4, “Regulatory Analysis: The Presumption Against Economic Regulation” [24].

  This document states that performance standards, rather than design standards, should be specified. The goal is to specify the requirements in terms of outcomes rather than specifying the means to those ends.

- OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources" [25].

  This appendix establishes a minimum set of controls to be included in federal automated information security programs; assigns federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123. Included in the appendix are security requirements for training, testing, incident response, technical controls, personnel security, and so on.
- The Federal Acquisition Regulation (FAR) [26] is the primary document that is used for the federal government. In addition, there are also department acquisition regulations (U.S. Department of Justice [DOJ], U.S. Department of Energy [DOE], U.S. Department of the Interior [DOI], U.S. Department of Defense [DOD]) and department/agency supplements (NASA, Air Force, DOD, U.S. Army Corps of Engineers). The Defense Federal Acquisition Regulations (DFAR) is used by DOD and the intelligence agencies. The FAR, and any associated supplements, are mandatory for federal agencies.
- As stated in the FAR:

  > Section 7.103: Agency-head responsibilities.
  > The agency head or a designee shall prescribe procedures for—
  > (w) Ensuring that agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544), OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology.

  DOD and the intelligence agencies are allowed exceptions to some of the requirements for other than full and open competition, for example, sole source, national security, international agreement, and public interest.

  Procurement guidance documents have been developed by NIST, U.S. Department of Homeland Security (DHS), DOJ, and so on. These guidance documents provide more specific interpretation of the general procurement documents.

  There are additional requirements for all procurements over $2 M and over $20 M.

- From Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities" [12]. http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf:

  U.S. Nuclear Licensee recommendations for implementing Cybersecurity for Critical Digital Assets.

  > RG 5.71 describes a regulatory position that promotes a defensive strategy consisting of a defensive architecture and a set of security controls based on standards provided in NIST SP 800-53 and NIST SP 800-82, "Guide to Industrial Control Systems Security," dated September 29, 2008 (Ref. 13). NIST SP 800-53 and SP 800-82 are based on well-understood cyber threats, risks, and vulnerabilities, coupled with equally well-understood countermeasures and protective techniques. Furthermore, NIST developed SP 800-82 for use within industrial control system (ICS) environments, including common ICS environments in which the information technology (IT)/ICS convergence has created the need to consider application of these security controls. RG 5.71 divides the above-noted security controls into three broad categories: technical, operational, and management.
  >
  > If a cyber attack were to result in the loss or degradation of safety, security, and emergency preparedness (SSEP) functions, the health and safety of the public might be at risk. Consequently, the U.S. Nuclear Regulatory Commission (NRC) developed this regulatory guide by tailoring the "high impact" baseline security controls described in NIST SP 800-53 and NIST SP 800-82 to provide an acceptable method to comply with 10 CFR 73.54. Where applicable, the NRC staff tailored the controls in NIST SP 800-53 and SP 800-82 to the unique environments of nuclear facility licensees and provided these more specific controls in Appendices A, B, and C to this document. The NRC's efforts to tailor the NIST baseline security controls are consistent with the recommendations provided in Appendix I to NIST SP 800-53 and in NIST SP 800-82. The process NIST used to develop these security controls was both peer reviewed and open to industry comment, and thus provides a well-established standard for cybersecurity which licensees should adopt to satisfy the regulatory requirement to defend digital assets from cyber attack up to and including the design basis threat (DBT), as defined in 10 CFR 73.1.

- Nuclear Energy Institute (NEI) 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors" [1]. Contact NEI www.nei.org to obtain a copy.

  NEI 08-09 has been developed to assist licensees in complying with the requirements of 10 CFR 73.54, "Physical Protection of Plants and Materials: Protection of Digital Computer and Communication Systems and Networks" [54] and RG 5.71. NEI 08-09 and RG 5.71 have converged in scope, and the NRC is expected to accept compliance with NEI 08-09 as equivalent to RG 5.71.

  NEI 08-09 describes a defensive strategy that consists of a defensive architecture and set of security controls that are based on the NIST SP 800-82, Final Public Draft, dated September 29, 2008, "Guide to Industrial Control Systems (ICS) Security" [20], and NIST SP 800-53, Revision 2, "Recommended Security Controls for Federal Information Systems and Organizations," standards. The security controls contained in NEI 08-09 Appendices D and E are tailored for use in nuclear facilities and are based on NIST SP 800-82 and NIST SP 800-53.

- NERC-CIP-002-009, North American Electric Reliability Corporation, "Cyber Security – Critical Cyber Asset Identification" [3], http://www.nerc.com/page.php?cid=2|20.

  This is a series of standards that include asset identification, security controls, and recovery plans for protection of critical cyber assets. It is not as detailed or as thorough as some of the other standards; however, most of the same categories are covered.

- IEC 61226, "Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions" [27]

  > International Electrotechnical Commission (IEC) 61226:2009 establishes a method of classification of the information and command functions for nuclear power plants, and the instrumentation and control (I&C) systems and equipment that provide those functions, into categories that designate the importance to safety of the function. The resulting classification then determines relevant design criteria. Is applicable to all the information and command functions and the I&C systems and equipment that provide those functions. The main changes with respect to the previous edition are listed below:
  > - to introduce a definition for "non-hazardous stable state"
  > - to clarify limits of categories
  > - to clarify requirements related to equipment used for beyond design events

- RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" [7] http://pbadupws.nrc.gov/docs/ML1028/ML102870022.pdf.

  This regulatory guide describes a method that the NRC staff deems acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for the use of digital computers in the safety systems of nuclear power plants. In this context, the term computer identifies a system that includes computer hardware, software, firmware, and interfaces.

- IEC/TS 62443-1-1 Edition 1.0 (2009-07-30), "Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models" [28]; IEC 62443-2-1 Edition 1.0 (2010-11-10), "Industrial Communication Networks – Network and System Security – Part 2-1: Establishing an Industrial Automation and Control System Security Program" [29]; IEC/TR 62443-3-1 Edition 1.0 (2009-07-30), "Industrial Communication Networks – Network and System Security – Part 3-1: Security Technologies for Industrial Automation and Control Systems" [30] http://webstore.iec.ch/webstore/webstore.nsf/mysearchajax?Openform&key=62443&sorting=&start=1&onglet=1

  This is a series of IEC standards publications about I&C cybersecurity.

  IEC/TS 62443-1-1:2009(E) is a technical specification that defines the terminology, concepts, and models for industrial automation and control systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series.

IEC 62443-2-1:2010(E) defines the elements necessary to establish a cybersecurity management system (CSMS) for IACS and provides guidance on how to develop those elements. The elements of a CSMS described in this standard are mostly related to policy, procedure, practice, and personnel, describing what shall or should be included in the final CSMS for the organization.

IEC/TR 62443-3-1:2009(E) provides a current assessment of various cybersecurity tools, mitigation countermeasures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control-system-centric cybersecurity technologies, the types of products available in those categories, the pros and cons of using those products in the automated IACS environments relative to the expected threats and known cyber vulnerabilities, and most important, the preliminary recommendations and guidance for using these cybersecurity technology products and/or countermeasures.

- IEC 62443-2-4, is a new proposed standard for cybersecurity procurement guidance.
- New TC 65 project working on a proposed standard based on the Working-party on Instrument Behavior (WIB) procurement guidance document. (see WIB in section C.3)
- ANSI/ISA-99, “Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program” [32] http://www.isa.org/standards

  ISA-99 provides a current assessment of security tools and technologies that apply to the manufacturing and control systems environment. It describes several categories of security technologies, the types of products available in those categories, the pros and cons of using those products in the manufacturing and control systems environment relative to expected threats and known vulnerabilities, and preliminary recommendations and guidance for using those security technologies.

  The ISA-99 series addresses electronic security within the industrial automation and control systems environment. The series serves as a foundation for the IEC 62443 series of the same titles as being developed by IEC TC65. See the full list of International Society of Automation (ISA) standards and reports in Figure C-1 from ISASecure.

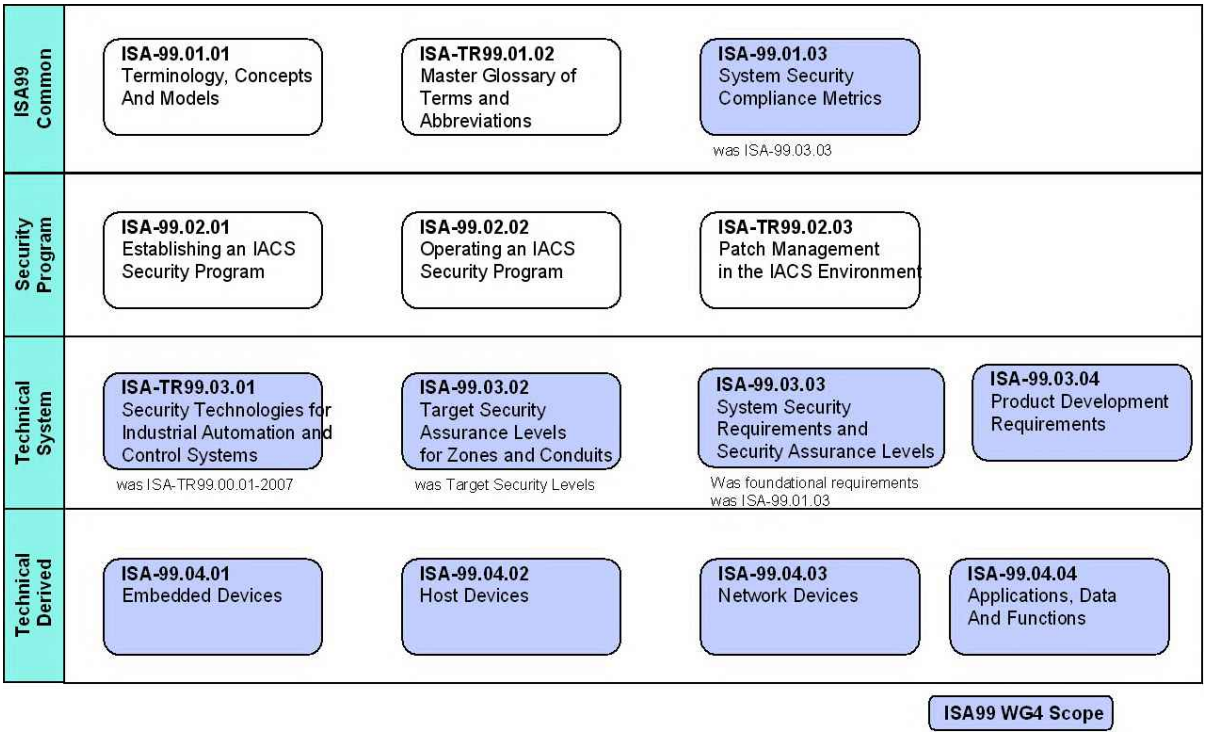

Figure C-1
ISA Standards and Reports
Courtesy of ISASecure

- IEC 62645 Edition 1.0, "Nuclear Power Plants – Instrumentation and Control Systems - Requirements for Security Programmes for Computer-Based Systems" [33]. New international nuclear cybersecurity standard in development, targeted for June 2012 http://www.iec.ch/dyn/www/f?p=103:38:0::::FSP_ORG_ID,FSP_LANG_ID,FSP_PROJECT:1358,25,IEC%2062645%20Ed.%201.0.

  This standard could be characterized as an international version of NEI 08-09. It specifically focuses on the issue of requirements for computer security programs and system development processes to prevent and/or minimize the impact of attacks against computer-based systems.

  This standard is being prepared and based on ISO/IEC 27000 series, International Atomic Energy Agency (IAEA), and country-specific guidance in this expanding technical and security focus area. It is intended that the standard be used by designers and operators of nuclear power plants (utilities), systems evaluators, vendors and subcontractors, and by licensors.

- International Atomic Energy Agency (IAEA), *International Atomic Energy Agency Reference Manual, Computer Security at Nuclear Facilities* [34] http://www-ns.iaea.org/security/infosec.asp?s=4.

  The publication aims at providing guidance specific to nuclear facilities on concerns, requirements and strategies for implementing a computer security program. This is achieved by presenting some authoritative approaches, structures, and implementation procedures designed for nuclear facilities. The publication also aims to provide advice on evaluating existing programs, assessing critical digital assets (CDAs), and identifying appropriate risk reduction measures.

- ISO/IEC 27000 Series; http://www.iso.org.
  - ISO/IEC 27000, "Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary" [35]
  - ISO/IEC 27001, "Information Technology – Security Techniques – Information Security Management Systems – Requirements" [36]
  - ISO/IEC 27002, "Information Technology – Security Techniques – Code of Practice for Information Security Management" [37]
  - ISO/IEC 27003, "Information Technology – Security Techniques – Information Security Management System Implementation Guidance" [38]
  - ISO/IEC 27004, "Information Technology – Security Techniques – Information Security Management – Measurement" [39]
  - ISO/IEC 27005, "Information Technology – Security Techniques – Information Security Risk Management" [40]
  - ISO/IEC 27006, "Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems" [41]
  - ISO/IEC 27011, "Information Technology – Security Techniques – Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002" [42]
  - ISO/IEC 27031, "Information Technology – Security Techniques – Guidelines for Information and Communications Technology Readiness for Business Continuity" [43]
  - ISO/IEC 27033, "Information Technology – Security Techniques – Network Security – Part 1: Overview and Concepts and Part 2: Guidelines for the Design and Implementation of Network Security" [44]
  - ISO 27799, "Health Informatics – Information Security Management in Health Using ISO/IEC 27002" [45]

  These international standards define the requirements and provide guidance for implementing an information security management system (ISMS). They also include guidance on auditing and provides a certification process. None of the interviewees mentioned ISO 27001 certification as a process or strategy that they have adopted or are pursuing, although the ISO 27000 series serves as a source document for other standards and guidance.

- ISO 28000, "Specification for Security Management Systems for the Supply Chain" [46] http://www.iso.org/.

  This document is a specification for security management systems for the supply chain including the requirements for a security management system, including those aspects critical to security assurance of the supply chain.
- DOD DIACAP (new), DITSCAP, *Department of Defense Information Assurance Certification and Accreditation Process.*

  DIACAP replaces the former process known as DITSCAP (*Department of Defense Information Technology Security Certification and Accreditation Process*) in 2006.

  Some DOD vendors have completed the DIACAP or DITSCAP certification process.

  DOD Instruction (DODI) 8510.01, "Department of Defense Information Assurance Certification and Accreditation Process (DOD DIACAP)" [55] establishes a standard DOD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an automated information system (AIS) that will maintain the information assurance (IA) posture of the defense information infrastructure (DII) throughout the system's life cycle.

  DIACAP applies to the acquisition, operation, and sustainment of any DOD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies the following four phases:

  1. System definition
  2. Verification
  3. Validation
  4. Reaccreditation

  DIACAP also uses weighted metrics to describe risks and their mitigation.

  The DIACAP processes were refined by the publication of the DIACAP "Application Manual" [56]. A similar methodology, National Information Assurance Certification and Accreditation Process (NIACAP), is used for the certification and accreditation (C&A) of national security systems outside of the DOD.

- EPRI report 1019187, *Technical Guideline for Cyber Security Requirements and Life Cycle Implementation Guidelines for Nuclear Plant Digital Systems* [47].
- EPRI report TR-106439, *Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications* [48].

C.2 Cybersecurity Guidance for Applying Standards

Interviewees indicated that they are using or are planning to use the following cybersecurity guidance for applying standards in the procurement of I&C critical assets:

- NEI 10-04, Revision 1, "Identifying Systems and Assets Subject to the Cyber Security Rule" http://www.nei.org/.

  The purpose of NEI 10-04 is to provide guidance on the identification of systems and assets subject to the requirements of 10 CFR 73.54 (NRC Cyber Security Rule), "Physical Protection of Plants and Materials: Protection of Digital Computer and Communication Systems and Networks" [54]. It is further identified as CDAs in RG 5.71.

- NEI 10-09 Revision 0, "Addressing Cyber Security Controls for Nuclear Power Reactors" (draft) http://www.nei.org/.

  This document (NEI 10-09) has been developed to ensure consistent understanding of the cybersecurity controls; ensure consistent understanding of the attack vectors associated with controls; describe a method to document and justify crediting existing programs, processes, and defensive architectures; and provide a consist methodology for addressing cybersecurity controls. These objectives are materialized in the development of a cybersecurity control implementation plan. A cybersecurity control implementation plan can enhance safe operations by supporting implementation consistency and reducing overall impact to site operations. The plan also acts to prepare licensees for inspections and for reviews of the implementation of the cybersecurity program.

  This new document is scheduled for release in mid-2011.

- ISASecure is an organization developed to provide a path for an accredited certification for devices and software development (www.isasecure.org), documentation, audit, and testing by accredited ISASecure test agencies to obtain certification. It is used to meet ISA-99 standards. ISA Security Compliance Institute (ISCI) developed ISASecure certifications specifications using the framework of the ISA-99 Standards Roadmap. The ISASecure program scope and direction are based on the security lifecycle concept for automation controls and are organized into the following three broad lifecycle phases:
  - Devices and systems: conform to ISASecure requirements (products constructed to secure characteristics and behaviors)
  - Supplier practices: product development life cycle (design for security)
  - User practices: integration/deployment, operations, and life cycle management (manage for security)

  The first ISASecure certification, Embedded Device Security Assurance (EDSA), focuses on the security of embedded devices and addresses device characteristics and supplier development practices for those devices.

  An embedded device that meets the requirements of the ISASecure EDSA specification earns the ISASecure EDSA certification, which is a trademarked designation that provides instant recognition of product security characteristics and capabilities, and

provides an independent industry stamp of approval similar to a Safety Integrity Level Certification (IEC EN 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems" [50]).

The ISASecure EDSA certification offers three levels of recognition for a device, reflecting increasing levels of device security assurance. The levels include ISASecure Level 1 for Devices, ISASecure Level 2 for Devices, and ISASecure Level 3 for Devices. All levels of security certification granted under this program contain the following technical elements:

- Functional security assessment (FSA)
- Software development security assessment (SDSA)
- Communication robustness testing (CRT)

- IAEA, Coordinated Research Project (CRP) on Cyber Security of Digital I&C Systems in Nuclear Power Plants, is a project similar to Electric Power Research Institute (EPRI) and NEI efforts but does not appear to address procurement guidance; it does, however, contemplate developing best practices.
- European Commission, *A Reference Security Management Plan for Energy Infrastructure,* European Programme for Critical Infrastructure Protection (EPCIP) [49] http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf.

  This document is a reference guide for developing an overall security management plan for energy infrastructure critical assets. The methodology in the guidebook is presented as a complete process supported by guidance notes and templates to assist a security manager in the development and implementation of a security management plan for a specific asset that not only fits within the overall risk management framework of the owner/operator but also reflects best-practice thinking on all aspects of risk identification, assessment, design, and implementation.
- IEC EN 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems" [50] http://www.iec.ch/functionalsafety/standards. This includes safety integrity level (SIL) and defines SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for **both** categories to achieve a given SIL.

  The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. To achieve a given SIL, the device must meet targets for the maximum probability of dangerous failure and a minimum safe failure fraction. The concept of "dangerous failure" must be rigorously defined for the system in question, normally in the form of requirement constraints whose integrity is verified throughout system development. The actual targets required vary depending on the likelihood of a demand, the complexity of the device(s), and types of redundancy used. Probability of failure on demand (PFD) and risk reduction factor (RRF) of low demand operation for different SILs are defined in IEC EN 61508.

C.3 Cybersecurity Procurement Guidance

Interviewees indicated that they are using or are planning to use the following cybersecurity procurement guidance in the procurement of I&C critical assets:

- WIB Report M 2784 X 10 Revision 2, "Process Control Domain – Security Requirements for Vendors" [15] http://www.wib.nl/.

  This control system procurement guidance document specifies requirements and gives recommendations for IT security to be fulfilled by vendors of control systems and automation systems. This was developed by commercial users and vendors for use in any application. There are specific language examples covering a comprehensive list of generic cybersecurity requirements, and it also gives sample language for factory acceptance test (FAT) and site acceptance test (SAT).

  There are gold, silver, and bronze levels of requirements. Commercial buyers and vendors are using this document as a guide for procurement specifications.
- Department of Homeland Security, *Cyber Security Procurement Language for Control Systems* [14] http://www.dhs.gov/files/cybersecurity.shtm.

  This document summarizes security principles that should be considered when designing and procuring control systems products and services (software, systems, maintenance, and networks), and it provides example language to incorporate into procurement specifications.

  It is a "tool kit" designed to reduce control systems cybersecurity risk. The tool kit includes a collection of security procurement language that maps directly to critical vulnerabilities observed in current and legacy control systems and that can be mitigated by technology providers and organizations through effective management of the technology across the systems' operational lifespan. It covers generic cybersecurity requirements and gives sample language for FAT and SAT.
- ISASecure: See the description in the previous section for details.
- IEC 62443-2-4, Proposed project to update IEC 62443 with IEC 62443-2-4 based on WIB for cybersecurity procurement guidance for general control systems.

The Electric Power Research Institute Inc., (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent more than 90 percent of the electricity generated and delivered in the United States, and international participation extends to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

1023502

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com