Cybersecurity Procurement Language for Energy Delivery Systems

April 2014

Energy Sector Control Systems Working Group (ESCSWG)

For Questions or Comments

Energy sector asset owners, operators, and suppliers are encouraged to provide feedback on this document to enhance the cybersecurity procurement language for future versions. Please send questions or comments to es-pl@energetics.com.

Acknowledgements

This document was prepared by the Energy Sector Control Systems Working Group (ESCSWG), Pacific Northwest National Laboratory (PNNL), and Energetics Incorporated, with funding from the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) Cybersecurity for Energy Delivery Systems (CEDS) program, and in collaboration with the U.S. Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Duke Energy, Edison Electric Institute (EEI), the Electric Power Research Institute (EPRI), the Federal Energy Regulatory Commission (FERC), the Independent Electric System Operator (IESO) in Ontario, and the Utilities Telecom Council (UTC). Contributions were also provided by the American Public Power Association (APPA), American Gas Association (AGA), and Idaho National Laboratory (INL).

A special thanks to Ed Goff of Duke Energy for his dedication and leadership in guiding this effort. Also, a special thanks to the many unlisted stakeholders and experts who provided comments and feedback during the two comment review periods for this document.

Disclaimer

This material was prepared as an account of work sponsored in part by an agency of the United States Government. Neither the ESCSWG, nor the United States Government nor any agency thereof, nor any of their employees, nor the technical contributors to this document or their employers, MAKES ANY WARRANTY, EXPRESSED OR IMPLIED, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information or processes disclosed, or represents that its use would not infringe privately owned rights.

Contents

For Questions or Comments i

Acknowledgements i

Disclaimer i

1. INTRODUCTION 1

1.1 Cybersecurity of Energy Delivery Systems 1

1.2 Background on Cybersecurity Procurement Language 1

1.3 Procurement Aligns with Energy Sector Cybersecurity Initiatives 2

1.4 About this Document 3

1.5 How to Use this Document 5

1.6 Examples of How to Use this Document 10

2. GENERAL CYBERSECURITY PROCUREMENT LANGUAGE 13

2.1 Software and Services 13

2.2 Access Control 14

2.3 Account Management 15

2.4 Session Management 16

2.5 Authentication/Password Policy and Management 16

2.6 Logging and Auditing 17

2.7 Communication Restrictions 18

2.8 Malware Detection and Protection 20

2.9 Heartbeat Signals 21

2.10 Reliability and Adherence to Standards 21

3. THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM 23

3.1 Secure Development Practices 23

3.2 Documentation and Tracking of Vulnerabilities 24

3.3 Problem Reporting 25

3.4 Patch Management and Updates 26

3.5 Supplier Personnel Management 27

3.6 Secure Hardware and Software Delivery 27

4. INTRUSION DETECTION 29

4.1 Host Intrusion Detection 29

4.2 Network Intrusion Detection 29

5. PHYSICAL SECURITY 31

5.1 Physical Access to Energy Delivery System Components 31
5.2 Perimeter Access 31
5.3 Communications inside the Physical Security Perimeter 32
6. WIRELESS TECHNOLOGIES 33
6.1. General Wireless Technology Provisions 33
7. CRYPTOGRAPHIC SYSTEM MANAGEMENT 34
7.1. Cryptographic System Documentation 34
7.2. Cryptographic Key and Method Establishment, Usage, and Update 34
8. REFERENCES 36
9. ABBREVIATIONS AND ACRONYMS 39
10. GLOSSARY 41
11. ADDITIONAL ACKNOWLEDGEMENTS 42

1. INTRODUCTION

1.1 Cybersecurity of Energy Delivery Systems

Energy delivery systems are critical to the effective and reliable operation of North America's energy infrastructure. Our twenty-first-century way of life is made possible by the vast network of processes enabled by these systems, as well as the interconnected electronic components, communication devices, and people who monitor and control those processes. Energy delivery systems are used to monitor and control the production, transfer, and distribution of energy. These systems include Supervisory Control and Data Acquisition (SCADA) systems, Energy Management Systems (EMSs), Distribution Management Systems (DMSs), and Distributed Control Systems (DCSs). Energy delivery systems comprise the following:

- The sensors and actuators used for monitoring and controlling energy delivery processes.
- The computer-based systems that analyze and store data.
- The communication pathways and networks that interconnect the various computer systems.

Cybersecurity threats, whether malicious or unintentional, pose a serious and ongoing challenge for the energy sector. Today's highly reliable and flexible energy infrastructure depends on the ability of energy delivery systems to provide timely, accurate information to system operators and automated control over a large, dispersed network of assets and components. A cyberattack on an energy delivery system can have significant impacts on the availability of a system to perform critical functions as well as the integrity of the system and the confidentiality of sensitive information. This, in turn, could impact national security, public safety, and the economy.

A variety of steps need to be taken throughout the life cycle of energy delivery systems to protect them from cyber threats. Embedding cybersecurity in the procurement of energy delivery systems is an important step for protecting these systems and is the focus of this document. Including cybersecurity in the procurement process can ensure that those purchasing and supplying energy delivery systems consider cybersecurity starting from the design phase of system development. This further ensures that cybersecurity is implemented throughout the testing, manufacturing, delivery, installation, and support phases of the product life cycle, improving overall reliability and reducing cybersecurity risks. To assist with embedding cybersecurity in the procurement of energy delivery systems, this document provides baseline cybersecurity procurement language for use by asset owners, operators, integrators, and suppliers during the procurement process.

1.2 Background on Cybersecurity Procurement Language

The U.S. Department of Energy (DOE) and the U.S. Department of Homeland Security (DHS) collaborated with industry cybersecurity and control system subject matter experts to publish *Cyber Security Procurement Language for Control Systems* in 2009 (henceforth referred to as DHS [2009]). The development of DHS (2009) brought together leading control system security experts, asset owners and operators, integrators, and suppliers across many sectors (e.g., electricity, natural gas, petroleum and oil, water, transportation, and chemical), as well as representatives from federal and state governments and international stakeholders.

The DHS (2009) document summarizes security principles and controls to consider when designing and procuring control system products and services (e.g., software, systems, maintenance, and networks), and provides example language that could be incorporated into procurement specifications. The document was intended as a "toolkit" to reduce energy delivery systems' cybersecurity risk by asking suppliers to assist in managing known vulnerabilities and deliver more secure systems.

The information provided in DHS (2009) was not intended to replace the application of good engineering practices or judgment; instead, the intent was to encourage suppliers and acquirers of energy delivery systems to work together to identify risk mitigation strategies specific to their system(s). It built on the premise that an energy delivery system's prime functions, design, and expected behaviors need to be considered prior to adding or requesting security features through the procurement process.

1.3 Procurement Aligns with Energy Sector Cybersecurity Initiatives

Several efforts have been developed and are underway in the energy sector to help address the evolving cybersecurity challenges faced by the sector. This procurement language document complements other cybersecurity efforts by providing organizations that acquire, integrate, and supply energy delivery systems with guidance on how to communicate cybersecurity expectations in a clear and repeatable manner.

The *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, developed by the Energy Sector Control Systems Working Group (ESCSWG) in 2011, provides a common vision and strategic framework to guide industry and government partnerships that will secure energy delivery systems. The roadmap vision is that by 2020, these systems will be designed, installed, operated, and maintained to survive a cyber incident while sustaining critical energy delivery functions. The roadmap's strategic framework includes strategies and milestones linked to distinct time frames for completion to help guide coordinated energy sector efforts. Including cybersecurity in the procurement process aligns with the roadmap's vision and strategy to build a culture of security, helping to make cybersecurity practices reflexive and expected among energy sector stakeholders.

In addition, the Cybersecurity Capability Maturity Model (C2M2) was designed to improve energy sector cybersecurity capabilities and provide a means for organizations to prioritize cybersecurity investments. This model was developed in support of a White House initiative and was led by DOE, in partnership with DHS, through a public-private partnership involving industry subject matter experts and other representatives from the public and private sectors. The C2M2 program has produced an evaluation tool to help organizations assess the maturity of their cybersecurity capabilities. Consideration of supply chain issues and cybersecurity procurement are elements of the maturity model. By utilizing the baseline cybersecurity procurement language identified in this procurement language document, utilities can improve their cybersecurity maturity level. The C2M2 program supports three versions of the model—a version for the electricity subsector, a version for the oil and natural gas subsector, and a version that is agnostic of an organization's role in critical infrastructure.

The Electricity Subsector Cybersecurity Risk Management Process (RMP) provides an approach for energy sector organizations, particularly in the electricity subsector, to manage cybersecurity risk in a consistent and repeatable manner. Developed by the DOE Office of Electricity Delivery and Energy

Reliability (OE), the National Institute of Standards and Technology (NIST), and the North American Electric Reliability Corporation (NERC), the RMP was written to enable energy sector organizations—regardless of their size or internal structure—to apply and tailor effective and efficient risk management processes to their organizational requirements. Risks associated with the acquisition of information technology (IT) and industrial control systems are included in the RMP. This procurement language document can help asset owners manage their cybersecurity risks by requesting cybersecurity features prior to acquisition.

Finally, NIST's *Framework for Improving Critical Infrastructure Cybersecurity* identifies a common language to address and manage cybersecurity risk in a cost-effective way based on business needs. Developed in collaboration between government and the private sector in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," the voluntary framework focuses on business drivers to guide cybersecurity activities. The Framework includes a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors. Specific cybersecurity activities focus on identifying and communicating an organization's role in the supply chain as well as managing cybersecurity risks with third-party stakeholders. The Framework also presents a common language that may be leveraged by those involved in the procurement process. This procurement language document can be used as a tool to help communicate cybersecurity requirements for the different categories of users in the procurement process, as identified in Table 1.

1.4 About this Document

Since 2009, the energy sector has continued to evolve as it faces new cybersecurity threats, advancing technologies, and increasingly stringent cybersecurity requirements and practices. In order to help energy sector asset owners and operators communicate expectations and requirements in a clear and repeatable manner, the ESCSWG built upon DHS (2009) to develop the baseline cybersecurity procurement language provided in this document. This language is tailored to the specific needs of the energy sector in order to provide a starting point for energy sector cybersecurity procurements. However, as the cybersecurity landscape continues to evolve, new threats, technologies, techniques, practices, and requirements may need to be considered during the energy sector procurement process. This document will also need to evolve to meet the challenges of this changing landscape.

The ESCSWG—a public-private partnership consisting of asset owners, operators, and government agencies—led the development of this document. Representatives from the ESCSWG, PNNL, and Energetics Incorporated worked closely with asset owners and operators, research institutes, trade associations, national laboratories, and suppliers representing the electricity and oil and natural gas subsectors in developing this document. Additionally, feedback was collected from energy sector stakeholders and cybersecurity experts, including acquiring organizations (representing large and small utilities), integrators, vendors, suppliers, consultants, standards organizations, regulators, and cybersecurity researchers during two stakeholder review periods.

Document Overview

This document provides baseline cybersecurity procurement language that is the consensus opinion of the document authors and was guided by input from voluntary reviewers representing the Acquirer, Integrator, and Supplier communities. It focuses on the cybersecurity of energy delivery systems (i.e., control systems) and does not attempt to specify or replace cybersecurity-based procurement language for acquisitions involving IT. Considerations for IT cybersecurity are outlined in many standards and guidance documents (e.g., the NIST 800 series of publications). Users of this document have the responsibility of ensuring that actions taken during the procurement process comply with current standards and regulations. In addition to the language included in this document, acquired products and services should conform to the applicable IT security standards and operations technology (OT) standards for energy delivery systems.

This document is designed to provide baseline cybersecurity procurement language for the following:

- Individual components of energy delivery systems (e.g., programmable logic controllers, digital relays, or remote terminal units).
- Individual energy delivery systems (e.g., a SCADA system, EMS, or DCS).
- Assembled or networked energy delivery systems (e.g., an electrical substation [transmission and distribution] or a natural gas pumping station).

This document intends to cover a broad range of energy delivery system procurements. The document differentiates the cybersecurity-based procurement language that is common to the procurement of individual components *and* systems from language that is only applicable to individual components *or* systems. Furthermore, this document differentiates language that is applicable to specific technologies (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP] communication between systems or components, and remote access capabilities).

Section 2 provides general cybersecurity considerations that apply to many types of products being procured as part of an energy delivery system, except where noted. The language should be tailored by the Acquirer based on the specific product being procured and the environment in which it will be integrated or applied. The section is grouped into the following topic areas:

- Software and Services
- Access Control
- Account Management
- Session Management
- Authentication/Password Policy and Management
- Logging and Auditing
- Communication Restrictions
- Malware Detection and Protection
- Heartbeat Signals
- Reliability and Adherence to Standards

Section 3 focuses on the Supplier's product life cycle security program, which should cover a product's design, development, manufacture, storage, delivery, implementation, maintenance, and disposal. A

properly designed and implemented security program should lower the risk that the Supplier's products will present major cybersecurity challenges for the Acquirer. The material presented in this section is grouped into the following topic areas:

- Secure Development Practices
- Documentation and Tracking of Vulnerabilities
- Problem Reporting
- Patch Management and Updates
- Supplier Personnel Management
- Secure Hardware and Software Delivery

Section 4 provides additional language to consider when acquiring intrusion detection systems, Section 5 focuses on physical security considerations, Section 6 focuses on wireless technologies, and Section 7 examines cryptographic technology.

Section 8 provides suggested references for review in addition to this document; however, this section does not attempt to list all relevant resources. Section 9 provides a list of abbreviations and acronyms used in this document, and Section 10 provides a suggested list of sources for common terms and definitions used in this document. Acquirers should review relevant sources including, but not limited to, the Internet Engineering Task Force (IETF) Glossary, National Institute of Standards and Technology Interagency Report (NISTIR) 7628, NIST 800-82, International Electrotechnical Commission (IEC) 62443, and NERC Critical Infrastructure Protection (CIP) standards for common terms and definitions. Section 11 acknowledges individuals who helped write or contributed to the development of this document.

1.5 How to Use this Document

Key Definitions

Table 1 provides definitions of the key terms used throughout this document to describe the three broad categories of procurement language users: the "Acquirer" (e.g., purchaser or buyer); the "Supplier" (e.g., vendor, seller, or manufacturer); and the "Integrator," who has a varying role and may act as an Acquirer and/or a Supplier.

Table 1. Definitions for the Different Categories of Procurement Language Users

Procurement Language User	Definition	Source
Acquirer	Stakeholder that acquires or procures a product or service.	ISO/IEC 15288, adapted
Supplier	Organization or individual that enters into an agreement with the Acquirer or Integrator for supplying a product or service. This includes all Suppliers in the supply chain.	ISO/IEC 15288, adapted
Integrator	An organization that customizes (e.g., combines, adds, or optimizes) components, systems, and corresponding processes. The integrator function can be performed by the Acquirer, the Supplier, or an independent third party. Conversely, an Integrator may function as an Acquirer and/or a Supplier when developing systems and components for deployment. Therefore, references to Acquirers and Suppliers in this document pertain to Integrators performing those functions.	NISTIR 7622, adapted

Source: National Institute of Standards and Technology (NIST). *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (Gaithersburg, MD: National Institute of Standards and Technology, 2013), http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf.

Definitions of specific procurement language terminology included in this document are shown in Table 2.

Table 2. Definition of Procurement Language Terminology

Definition
The terms "shall" and "shall not" indicate that the procurement language element in which these terms appear is to be strictly followed if the Acquirer and Supplier agree to adopt the language in their procurement contract.
The terms "should" and "should not" indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.
The term "may" indicates a course of action permissible within the limits of the document.
The terms "can" and "cannot" indicate the possibility of something occurring.
The term "procured product" may refer to the hardware, software, and firmware that compose the energy delivery system, or a component thereof, that is being acquired through the procurement process. This may also refer to support and maintenance services that are being acquired through the procurement process.

Summary of How to Use this Document

This document is intended for use by the following:

- Acquirers seeking to incorporate cybersecurity into the procurement of energy delivery systems or components. Requests or specifications may be issued by the Acquirer through requests for proposal (RFPs) or requests for information (RFIs).

- Acquirers seeking to evaluate the cybersecurity maturity of energy delivery systems or components offered by Suppliers and Integrators.
- Suppliers and Integrators designing or manufacturing systems, components, and services that will meet cybersecurity features requested by Acquirers (or in some cases, Integrators).
- Acquirers, Integrators, and Suppliers negotiating procurement contracts that outline cybersecurity features and responsibilities for each party involved in the procurement.

The procurement language presented in this document is *not* intended to be inserted (or attached) directly or verbatim into a procurement contract. Specific language that is appropriate for the applicable procurements should be negotiated by the Acquirer and Supplier based on the system, component, or service and the intended application of the energy delivery system in accordance with the cybersecurity risk tolerance of the Acquirer. Specific procurement language should be agreed upon by both the Acquirer's and Supplier's contracting offices.

Figure 1 features a summary of key points on how to use this document. These points are further explained in the latter part of this section.

Figure 1. Summary of Key Points on How to Use this Document

Overview

- The cybersecurity-related procurement language in this document is intended for use by Acquirers, Integrators, and Suppliers.
- The procurement language presented in this document is *not* intended to be inserted (or attached) directly or verbatim into a procurement contract. The Acquirer and Supplier will need to involve their respective contracting offices in selecting and customizing their procurement contract language.

Adding Procurement Language

- Acquirers may go beyond the baseline procurement language listed in this document when preparing an RFP or an RFI. Additionally, Suppliers may go beyond this baseline language when proposing products or services in response to an RFP or an RFI.

Modifying Procurement Language

- Cybersecurity procurement language may be modified per agreement between the Acquirer and Supplier to meet the specific procurement.
- Procurement language should only be included in contracts if it could reduce security risk or provides value. If the Acquirer and Supplier agree that a specific element of the language may not reduce security risk or does not add value, it may be dropped or replaced by alternative language that achieves a comparable security objective.

Negotiating Procurement Language

- In negotiating procurement language, this document can be used to identify those features that are "must haves" for the Acquirer as well as those that may be discretionary and can be negotiated.

Procurements with Integrators and Multiple Suppliers

- When an energy delivery system contains components from multiple Suppliers, additional cybersecurity procurement language may be required to ensure the secure delivery and integration of those components.

Applicability of Procurement Language

- Unless otherwise specified, the procurement language in this document applies "at the point of delivery" of the product.
- Features needed for operation of a product include those features needed for routine, emergency, or maintenance operations and product testing after delivery.

Adding Procurement Language

The baseline procurement language presented in this document is *not* intended to be all-inclusive. Different products and services may be used for different applications and may require additional cybersecurity-based procurement language that has not been identified in this document. Therefore, Acquirers may go beyond the baseline procurement language listed in this document when preparing an RFP or an RFI. Acquirers should review other resources provided by entities including, but not limited to, NIST, NERC, DHS, SANS, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the Institute of Electrical and Electronics Engineers (IEEE), the International Society of Automation (ISA), the International Organization for Standardization (ISO), and IEC, which may provide additional information or cybersecurity language pertaining to a specific procurement. There are also some explicit, mandatory compliance standards (e.g., NERC CIP standards) that should be evaluated by Acquirers as sources of potential requirements. This document does not attempt to identify or list all such resources. Some suggested resources that may be considered are listed in the References (Section 8).

Suppliers may also go beyond this baseline cybersecurity procurement language when proposing products or services in response to an RFP or an RFI. The specific features of these products and services may be documented as additional cybersecurity language in the procurement contract. The Supplier may also propose cybersecurity features for the Acquirer to safeguard sensitive Supplier product information or to clarify cybersecurity responsibilities that need to be assumed by the Acquirer. This document does not include cybersecurity procurement language specific to the Acquirer.

Modifying Procurement Language

Energy delivery system environments, technologies, and risks vary. Therefore, the cybersecurity language for the procurement of a particular product should be tailored according to the relevant cybersecurity programs and policies of the environment into which the product will be integrated or applied. Acquirers, Suppliers, and Integrators may modify language as needed to account for the specific design of a product, the architecture into which it will be installed, or the existing risk management employed by the Acquirer or Supplier.

In some cases, procurement language that is listed as applying more broadly to energy delivery system acquisitions may not be appropriate for a particular application (examples of this are provided in Section 1.6). There will be procurements in which the Acquirer and Supplier agree that a given feature is not appropriate.

Procurement language should only be included in contracts if it could reduce security risks or provide value. If the Acquirer and Supplier agree that a specific element of the language may not reduce risk, does not add value, or results in unnecessary complexity, it may be dropped or replaced by alternative language that provides an appropriate approach for achieving the desired security objective. Procurement language should be customized for the Acquirer's environment to avoid any inadvertent impacts on required safety features or essential functionality of the energy delivery system or component.

It is recommended that any procurement language provided in this document that is replaced, dropped, or extensively modified be documented and captured as part of the Acquirer's risk management program. Any resulting cybersecurity risk impacts should also be noted. Having a record of this decision will assist the Acquirer in future procurement activities and support risk monitoring activities.

Negotiating Procurement Language

When negotiating cybersecurity-based procurement language, Acquirers and Suppliers may have different opinions on the merits and applicability of specific elements of the language in this document. An Acquirer may benefit from speaking with multiple Suppliers during the procurement process to identify those who can offer products and services with enhanced cybersecurity that best meet the Acquirer's procurement needs. By providing baseline cybersecurity procurement language, this document can be used to identify those features that are "must haves" for the Acquirer and those that may not apply.

Procurements with Integrators and Multiple Suppliers

This document does not distinguish between procurement language that may be specific to a Supplier or an Integrator. Acquirers should consider whether the functions being requested are to be performed by a Supplier or an Integrator, and then adjust their contract language as appropriate for each. In some cases, specific language may apply to both Suppliers and Integrators.

Additionally, Acquirers should consider the cybersecurity implications of acquiring components of an energy delivery system from multiple Suppliers. Maintaining appropriate cybersecurity in such a system may require additional language that ensures the secure integration of components, including hardware, software, and firmware from multiple Suppliers.

Applicability of Procurement Language

Unless otherwise specified, the procurement language in this document is intended to apply "at the point of delivery" of the product. Service and support provided by the Supplier may apply, as indicated, well after the delivery of the product. Some aspects of the Supplier's product life cycle security program apply well before and well after the delivery of the product.

References to hardware, software, and firmware features needed for operation of the product include those features needed for routine, emergency, or maintenance operations and product testing after delivery. They do not refer to features that are no longer needed after product delivery.

1.6 Examples of How to Use this Document

This subsection provides specific examples that demonstrate how Acquirers and Suppliers may exhibit flexibility when applying the procurement language presented in this document.

Inapplicable Procurement Language

In some instances, this document provides procurement language that the Acquirer and Supplier may mutually agree is not applicable for the given situation; for example, Item 3 in Section 2.4:

2.4.3 The Supplier shall not, unless specifically requested by the Acquirer, allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins, unless specifically requested by the Acquirer.

If a procured product requires multiple concurrent logins using the same authentication credentials to support its intended operation, the Acquirer and Supplier may determine this is acceptable for a given solution. To compensate, the Acquirer may wish to implement security controls (e.g., enhanced physical security or the disabling of remote access) as part of the procurement or as a separate activity. The Acquirer should document the decision to drop this procurement language and record it in the Acquirer's security risk management system. In addition, the Acquirer should document a description of any compensating security controls that offset the risks associated with dropping this procurement language.

Another example of procurement language that the Acquirer and Supplier may mutually agree is not applicable for a given application is Item 1 in Section 2.9:

2.9.1 *The Supplier shall identify heartbeat signals or protocols and recommend which should be included in network monitoring. At a minimum, a last gasp report from a dying component or equivalent shall be included in network monitoring.*

There are procurements where heartbeat signals may not be applicable. The Acquirer and Supplier may identify other appropriate approaches for monitoring the health, performance, or security status of networked devices. The Acquirer should document the decision to drop this language and record it in the Acquirer's security risk management system. If alternative security controls are adopted instead, the Acquirer should also document them.

Specifying Periods of Applicability

The procurement language included in this document is intended for the period of the contract, which will depend on the type of contract mechanism being used. However, there is specific procurement language where the period of applicability may need to be negotiated between the Acquirer and Supplier. For example, Item 2 in Section 3.3 states the following:

3.3.2 Upon the Acquirer submitting a problem report to the Supplier, the Supplier shall review the report, develop an initial action plan within [a negotiated time period], and provide status reports of the problem resolution to the Acquirer within [a negotiated time period].

Acquirers should fill in the time period requested within the brackets before issuing an RFP or an RFI. This time period should meet the needs of the Acquirer. The Acquirer and Supplier will need to negotiate a mutually acceptable time period to include in the final contract.

The Scope of Documentation or Verification

A number of procurement language elements request summary documentation or verification from the Supplier. For example, Item 6 in Section 2.1 states the following:

2.1.6 *The Supplier shall provide summary documentation of procured product's security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.*

Acquirers may wish to request more detailed documentation if it is needed to ensure their cybersecurity expectations are met.

Procurement language that requests documentation or summary documentation may drift into areas that involve sensitive information that a Supplier does not wish to fully disclose to its customers or the public. For example, Item 3 in Section 2.7 states the following:

2.7.3 *The Supplier shall provide a method to restrict communication traffic between different network security zones. The Supplier shall provide documentation on any method or equipment used to restrict communication traffic.*

This procurement language is not intended to require the Supplier to provide sensitive information to the Acquirer. If the Supplier determines that the requested information is sensitive, the Acquirer and Supplier will need to negotiate how to proceed. An agreement may be reached that the information provided to the Acquirer will be "sanitized" to meet the Acquirer's information needs and the Supplier's need to protect its sensitive information. Alternatively, the Supplier can propose procurement language stating that the Acquirer will need to maintain an appropriate information security program that securely maintains any sensitive information provided to the Acquirer.

2. GENERAL CYBERSECURITY PROCUREMENT LANGUAGE

This section presents cybersecurity-based procurement language for the product(s) being acquired that may be generally applicable to a single component of an energy delivery system, a complete energy delivery system, or a set of integrated energy delivery systems. Prior to being used for procurement contracts, this language should be tailored to the specific component or system, or to the integrated set of systems that work together to perform a major energy delivery function.

2.1 Software and Services

Unused and unnecessary software and services in energy delivery systems and components that are left enabled can pose potential entry points for exploits, especially if they are not monitored. These services can range from system diagnostics to chat programs. Various attacks have been crafted to exploit these vulnerabilities, leading to the compromise. These vulnerabilities can be addressed by the "principle of least functionality," which states that programs or processes must only be able to access the information and computational resources that are needed for them to perform their intended function.

Baseline procurement language:

2.1.1. The Supplier shall remove all software components that are not required for the operation and/or maintenance of the procured product. If removal is not technically feasible, then the Supplier shall disable software not required for the operation and/or maintenance of the procured product. This removal shall not impede the primary function of the procured product. If software that is not required cannot be removed or disabled, the Supplier shall document a specific explanation and provide risk mitigating recommendations and/or specific technical justification. The Supplier shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but not be limited to:

- Games
- Device drivers for product components not procured/delivered
- Messaging services (e.g., email, instant messenger, peer-to-peer file sharing)
- Source code
- Software compilers in user workstations and servers
- Software compilers for programming languages that are not used in the energy delivery system
- Unused networking and communications protocols
- Unused administrative utilities, diagnostics, network management, and system management functions
- Backups of files, databases, and programs used only during system development
- All unused data and configuration files

2.1.2. The Supplier shall provide documentation of software/firmware that supports the procured product, including scripts and/or macros, run time configuration files and

interpreters, databases and tables, and all other included software (identifying versions, revisions, and/or patch levels, as delivered). The listing shall include all ports and authorized services required for normal operation, emergency operation, or troubleshooting.

2.1.3. The Supplier shall remove and/or disable, through software, physical disconnection, or engineered barriers, all services and/or ports in the procured product not required for normal operation, emergency operations, or troubleshooting. This shall include communication ports and physical input/output ports (e.g., USB docking ports, CD/DVD drives, video ports, and serial ports). The Supplier shall provide documentation of disabled ports, connectors, and interfaces.

2.1.4. The Supplier shall configure the procured product to allow the Acquirer the ability to re-enable ports and/or services if they are disabled by software.

2.1.5. The Supplier shall disclose the existence of all known methods for bypassing computer authentication in the procured product, often referred to as backdoors, and provide written documentation that all such backdoors created by the Supplier have been permanently deleted from the system.

2.1.6. The Supplier shall provide summary documentation of the procured product's security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.

2.2 Access Control

Products that do not have appropriate access control methods in place can allow adversaries to gain unauthorized or undetected access to systems. Access control is the process of restricting access to certain systems, information, functions, tools, locations, components, or resources. Access control limits individual users and processes by implementing the "principle of least privilege" so that every process, program, or user shall only access the information and resources for which it is authorized and that are necessary for operation. This reduces the number of potential entry points for an attack. Access control is designed to enforce security policies and streamline security management processes by grouping users based on their role within the organization, rather than separately evaluating each individual identity.

Baseline procurement language:

2.2.1. The Supplier shall configure each component of the procured product to operate using the principle of least privilege. This includes operating system permissions, file access, user accounts, application-to-application communications, and energy delivery system services.

2.2.2. The Supplier shall provide user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used.

2.2.3. The Supplier shall provide a system administration mechanism for changing user(s') role (e.g., group) associations.

2.2.4. The Supplier shall configure the procured product such that when a session or interprocess communication is initiated from a less privileged application, access shall be limited and enforced at the more critical side.

2.2.5. The Supplier shall provide a method for protecting against unauthorized privilege escalation.

2.2.6. The Supplier shall document options for defining access and security permissions, user accounts, and applications with associated roles. The Supplier shall configure these options, as specified by the Acquirer.

2.2.7. The Supplier shall recommend methods for the Acquirer to prevent unauthorized changes to the Basic Input/Output System (BIOS) and other firmware. If it is not technically feasible to protect the BIOS to reduce the risk of unauthorized changes, the Supplier shall document this case and provide mitigation recommendations.

2.2.8. The Supplier shall verify and provide documentation for the procured product, attesting that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones), as specified by the Acquirer.

2.2.9. The Supplier shall deliver a product that enables the ability for the Acquirer to configure its components to limit access to and from specific locations (e.g., security zones, business networks, and demilitarized zones [DMZs]) on the network to which the components are attached, where appropriate, and provide documentation of the product's configuration as delivered.

2.3 Account Management

Many energy delivery systems are configured with default accounts and passwords that are sometimes publicly available. In some cases, these accounts can be used to gain unauthorized system access or to escalate privileges.

Baseline procurement language:

2.3.1. The Supplier shall document all accounts (including, but not limited to, generic and/or default) that need to be active for proper operation of the procured product.

2.3.2. The Supplier shall change default account settings to Acquirer-specific settings (e.g., length, complexity, history, and configurations) or support the Acquirer in these changes. The Supplier shall not publish changed account information. The Supplier shall provide new account information to the Acquirer via a protected mechanism.

2.3.3. Prior to delivery of the procured product to the Acquirer, the Supplier shall remove or disable any accounts that are not needed for normal or maintenance operations of the energy delivery system.

2.3.4. As specified by the Acquirer, accounts for emergency operations shall be placed in a highly secure configuration and documentation on their configuration shall be provided to the Acquirer.

2.4 Session Management

Weak or insecure system session operating practices can result in vulnerabilities in energy delivery systems. Examples of insecure practices include permitting use of clear text passwords, passwords lacking requisite complexity, multiple concurrent session logins, remembered account information between logins, and auto-filling fields during logins. Once an account is compromised, system administrators have no way of knowing with certainty whether the account is being used by an unauthorized party.

Baseline procurement language:

2.4.1. The Supplier shall not permit user credentials to be transmitted or shared in clear text. The Supplier shall not store user credentials in clear text unless the Supplier and Acquirer agree that this is an acceptable practice for the procured product given the protection offered by other security controls. The Supplier shall only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through Secure Shell Terminal Emulation [SSH], Transport Layer Security [TLS]).

2.4.2. The Supplier shall provide an appropriate level of protection (e.g., encryption and digital signing) for the session, as specified by the Acquirer, commensurate with the technology platform, communications characteristics, and response time constraints.

2.4.3. Unless specifically requested by the Acquirer, the Supplier shall not allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.

2.4.4. The Supplier shall provide account-based and group-based configurable session-based logout and timeout settings (e.g., alarms and human-machine interfaces).

2.5 Authentication/Password Policy and Management

The need for constant availability of energy delivery systems often results in weak password policies, which can provide easy entry points into energy delivery systems. This may be caused by users selecting poor or easily guessed passwords that attackers can break within minutes.

Baseline procurement language:

2.5.1. The Supplier shall document the levels, methods, and capabilities for authentication and authorization. The Supplier shall deliver a product that adheres to standard authentication protocols.

2.5.2. The Supplier shall provide a configurable account password management system that allows for, but is not limited to, the following:

- Changes to passwords (including default passwords)
- Selection of password length
- Frequency of change
- Setting of required password complexity
- Number of login attempts prior to lockout
- Inactive session logout
- Screen lock by application
- Comparison to a library of forbidden strings
- Derivative use of the user name
- Denial of repeated or recycled use of the same password

2.5.3. The Supplier shall protect passwords, including not storing passwords in clear text and not hardcoding passwords into software or scripts.

2.5.4. The Supplier shall provide a centralized and local account management capability.

2.5.5. If needed for ongoing support and maintenance, the Supplier's solutions involving interactive remote access/control shall adhere to (i.e., be compatible with) the Acquirer's implementation of multifactor authentication (e.g., two-factor or token).

Baseline procurement language for secure single sign-on:

2.5.6. The Supplier shall ensure that account access for single sign-on is equivalent to that enforced as a result of direct login.

2.5.7. The Supplier shall use a secure method of authentication (e.g., strong two-factor authentication) to allow single sign-on to a suite of applications.

2.5.8. The Supplier shall protect key files and access control lists used by the single-sign-on system from non-administrative user read, write, and delete access. The single-sign-on system must resolve each individual user's credentials, roles, and authorizations to each application.

2.5.9. The Supplier shall provide documentation on configuring a single-sign-on system, as well as documentation showing equivalent results in running validation tests against the direct login and the single sign-on.

2.6 Logging and Auditing

Recording specific system activity in the form of logging generates an audit trail. Failure to perform logging makes it difficult to monitor activity, identify potential cyberattacks in time to take protective actions, perform diagnostics, and carry out forensic activities in the event of a successful cyberattack. Without easy access to information on system activity, post-event investigations may not yield conclusive results and the risk of similar events occurring in the future would remain high.

Baseline procurement language:

2.6.1. The Supplier shall provide logging capabilities or the ability to support the Acquirer's existing logging system. Logging capabilities provided by the Supplier shall be configurable by the Acquirer and support the Acquirer's security auditing requirements. As specified by the Acquirer, the procured product shall cover the following events, at a minimum (as appropriate to their function):

- Information requests and server responses
- Successful and unsuccessful authentication and access attempts
- Account changes
- Privileged use
- Application start-up and shutdown
- Application failures
- Major application configuration changes

2.6.2. The Supplier shall provide standard time synchronization in the procured product (e.g., Global Positioning System [GPS], Network Time Protocol [NTP], and IEEE 1508-2008). If the Supplier is not providing standard time synchronization and is providing an authoritative time source, the procured product shall be configured to synchronize to the authoritative time source.

2.6.3. The Supplier shall time stamp audit trails and log files, as specified by the Acquirer.

2.6.4. If required by the Acquirer, the Supplier shall provide confidentiality and integrity security protection of log files.

2.6.5. The Supplier shall implement an approach for collecting and storing (e.g., transfer or log forwarding) security log files.

2.6.6. The Supplier shall recommend log management and Security Information and Event Management (SIEM) integration methods (e.g., syslog).

2.6.7. The Supplier shall provide a list of all log management capabilities that the procured product is capable of generating and the format of those logs. This list shall identify which of those logs are enabled by default.

2.7 Communication Restrictions

Poorly designed network architectures that lack a defense-in-depth approach to security may be vulnerable to cyber exploitation. Security can be enhanced by partitioning networks into multiple segments and placing technical security controls (e.g., firewalls, unidirectional communication devices, or virtual private network [VPN] concentrators) between the network segments. Hardware, software, and firmware that restrict communications are important tools in establishing an appropriate cybersecurity defensive architecture. The network architecture is how a network is designed and segmented into logical, smaller functional subnets (i.e., network security zones) for the purpose of communication.

Baseline procurement language for the acquisition of networked energy systems:

2.7.1. The Supplier shall recommend guidance on the design and configuration of network security zones within the procured product.

2.7.2. The Supplier shall provide information on all communications (e.g., protocols) required between network security zones, whether inbound or outbound, and identify each network component of the procured product initiating communication.

2.7.3. The Supplier shall provide a method to restrict communication traffic between different network security zones. The Supplier shall provide documentation on any method or equipment used to restrict communication traffic.

2.7.4. The Supplier shall verify and document that disconnection points are established between the network security zones and provide the methods to isolate the zones to continue limited operations.

2.7.5. The Supplier shall provide a means to document that network traffic is monitored, filtered, and alarmed (e.g., alarms for unexpected traffic through network security zones) and provide filtering and monitoring rules.

2.7.6. If firewalls are provided by the Supplier, the Supplier shall provide documentation on the firewalls and their firewall rule sets for normal and emergency operations. If the Acquirer has the responsibility of procuring its own firewalls, the Supplier shall recommend appropriate firewall rule sets or rule set guidance for normal and emergency operations. The basis of the firewall rule sets shall be "deny all," with exceptions explicitly identified by the Supplier.

2.7.7. The Supplier shall provide the Acquirer with access, including administrative as needed, to network components of the procured product, including firewalls.

2.7.8. The Supplier shall document all remote access entry pathways and ensure that they can be enabled or disabled by the Acquirer as needed.

2.7.9. The Supplier shall verify that the procured product allows use of unique routable network address spaces (i.e., address spaces other than 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 must be supported) that work within the Acquirer's network. Where this is not available, the Supplier shall offer an alternative approach, with mitigating security measures, that is acceptable to the Acquirer.

Baseline procurement language for products that utilize communication tunneling (e.g., using a VPN):

2.7.10. The Supplier shall provide or utilize an existing security-isolated environment outside the control network (e.g., using a demilitarized zone [DMZ] or an equivalent or a superior form of security isolation) for the communications tunneling server to reside in.

2.7.11. The Supplier shall use different authentication credentials from those used for in-network communications when establishing control network access using communication tunneling.

2.7.12. The Supplier shall configure the communication tunneling components of the procured product (e.g., connectors, filters, and concentrators) to provide end-to-end protection (e.g., end-to-end encryption) of the data in transit. This shall address confidentiality and/or integrity, as specified by the Acquirer.

Baseline procurement language for the acquisition of energy delivery system networks or networking components:

2.7.13. The Supplier shall provide a method for managing the network components of the procured product and changing configurations, including hardware and software configurations (e.g., addressing schemes).

2.7.14. The Supplier shall verify and provide documentation that the network configuration management interface is secured.

2.7.15. The Supplier shall provide Access Control Lists (ACLs) for monitoring network components (e.g., port mirroring and network tap) of the procured product.

2.8 Malware Detection and Protection

Malicious code (e.g., malware) comes in many shapes and forms. Most often it is spread by humans via USB devices, email, or websites (by clicking) in the form of Trojans and viruses. Malicious code can enter systems through removable media. It can also be self-propagating in the form of worms. As energy delivery systems migrate onto Internet Protocol (IP)-based platforms, they become more susceptible to malware infections and require cyber protections against them.

Baseline procurement language for the acquisition of energy delivery systems and components with malware protection capabilities:

2.8.1. The Supplier shall provide, or specify how to implement, the capability to automatically scan any removable media that is introduced to the product being acquired.

2.8.2. The Supplier shall implement **at least one** of the following:

- Provide a host-based malware detection capability. The Supplier shall quarantine (instead of automatically deleting) suspected infected files. The Supplier shall provide an updating scheme for malware signatures. The Supplier shall test and confirm compatibility of malware detection application patches and upgrades.
- If the Supplier is not providing the host-based malware detection capability, the Supplier shall suggest malware detection products to be used and provide guidance on malware detection and configuration settings that will work with Supplier products.

- If the Supplier is not providing a host-based malware detection capability, nor suggesting malware detection products, and if specified by the Acquirer, the Supplier shall provide an application whitelisting solution that is tested, validated, and documented that shall only permit approved applications to run.

2.8.3. The Supplier shall validate that cybersecurity services running on the procured product (e.g., virus checking and malware detection) do not conflict with other such services running on the procured product.

2.9 Heartbeat Signals

Heartbeat signals are the regularly repeated signals generated by hardware, software, or firmware to indicate normal operation or for synchronization with other components within an energy delivery system. Heartbeat signals can be configured in the hardware, software, or firmware. If a heartbeat signal is not received in the prescribed time, it is an indication that the component generating the signal is not operating within its normal parameters. Heartbeat signals can be sent over serial connections or routed protocols. Problems may arise when heartbeat signals or protocols are corrupted, spoofed, or possibly used as an entry point for unauthorized access.

Baseline procurement language:

2.9.1. The Supplier shall identify heartbeat signals or protocols and recommend which should be included in network monitoring. At a minimum, a last gasp report from a dying component or equivalent shall be included in network monitoring.

2.9.2. The Supplier shall provide packet definitions of the heartbeat signals and examples of the heartbeat traffic if the signals are included in network monitoring.

2.10 Reliability and Adherence to Standards

Adherence to security standards is one step in protecting energy delivery systems and components from compromise. These standards should be considered when procuring energy delivery systems and components in order to improve security implementation, including the protection of sensitive information.

Baseline procurement language:

2.10.1. The Supplier shall protect the confidentiality and integrity of the Acquirer's sensitive information.

2.10.2. The Supplier shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput specified.

2.10.3. The Supplier shall use an implementation that complies with the current applicable interoperability and security standards, as specified by the Acquirer (e.g., NIST 800 series, ISA/IEC 62443, IEEE 1613, IEEE 1588, and NERC CIP).

2.10.4. Upon the Acquirer's request, the Supplier shall return or document the secure disposal of the Acquirer's data and Acquirer-owned hardware that is no longer needed by the Supplier (e.g., NIST Special Publication [SP] 800-80).

3. THE SUPPLIER'S LIFE CYCLE SECURITY PROGRAM

The Supplier's life cycle security program is an important consideration in the procurement process. Vulnerabilities frequently result from architecture, design, weaknesses, and vulnerabilities in hardware, software, and firmware coding, as well as in bundled third-party products. Many energy delivery system security vulnerabilities are the direct result of writing software with inadequate attention to secure coding practices that reduce the risk of successful deliberate and persistent malicious attacks. Life cycle security programs provide a structured way for developing robust products with fewer weaknesses and vulnerabilities or finding and remediating them before software and systems are delivered and installed in the Acquirer's environment. Supplier post-production support is critical for maintaining secure software and systems, including remediating newly discovered vulnerabilities and ensuring that spare parts can be replaced with genuine parts. Validating that hardware, software, or firmware has been delivered as it was ordered and shipped—without being tampered with or otherwise modified—is also important. After a product has been removed from service, the disposal of that product provides opportunities for the compromise of information and configurations that the Acquirer or Supplier may deem sensitive.

3.1 Secure Development Practices

Secure product development practices are a set of processes integrated into the system development life cycle (SDLC) that reduce the security risks of the overall product. These practices help to develop more robust hardware, software, and firmware with fewer weaknesses and vulnerabilities, as well as identify and remediate weaknesses and vulnerabilities before implementation. Secure development practices ensure that security is integrated into all phases of the SDLC and is considered a key component of system development.

Baseline procurement language:

3.1.1. The Supplier shall provide summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided energy delivery system hardware, software, and firmware. If applicable, the Supplier shall document how the most critical application security weaknesses (including *OWASP Top 10* or *SANS Top 25 Most Dangerous Software Errors*) are addressed in the Supplier's SDLC.

3.1.2. As specified by the Acquirer, the Supplier shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). The Supplier shall identify the countries where the development, manufacturing, maintenance, and service for the product are provided. The Supplier shall notify the Acquirer of changes in the list of countries where product maintenance or other services are provided in support of the procured product. This notification shall occur within [a negotiated time period] prior to initiating a change in the list of countries.

3.1.3. The Supplier shall provide a Quality Assurance program and validate that the software and firmware of the procured product have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. This testing shall include fuzz testing, static testing, dynamic testing, and penetration testing. The Supplier shall use positive and appropriate negative tests to verify that the procured product operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behavior during these tests. This testing may be done by the Supplier or an independent entity. The Supplier shall provide summary documentation of the results of the testing that includes unresolved vulnerabilities and recommended mitigation measures.

3.1.4. The Supplier shall provide summary documentation of its coding reviews, including defect lists and plans to correct identified vulnerabilities.

3.1.5. The Supplier shall communicate security-related technical issues with a single technical point of contact (e.g., a company support email address or a company support phone number), as specified by the Acquirer. The Supplier shall communicate with the Acquirer within [a negotiated time period] (see Section 3.3.3). This is not intended for non-technical contract-related issues.

3.1.6. The Supplier shall provide documentation of all input validation testing including, but not limited to, measures for prevention of command injection, Structured Query Language (SQL) injection, directory traversal, Remote File Include, Cross-Site Scripting (XSS), and buffer overflow.

3.1.7. The Supplier shall provide a contingency plan for sustaining the security of the procured product in the event the Supplier leaves the business (e.g., security-related procedures and products placed in escrow).

3.1.8. The Acquirer shall have the right to request documentation of the Supplier's implemented cybersecurity program, including recent assessment results or conduct periodic [at a negotiated frequency and scope] on-site security assessments at the Supplier's facilities. These on-site security assessments may be conducted by an independent third party, at the discretion of the Acquirer.

3.2 Documentation and Tracking of Vulnerabilities

When security vulnerabilities are discovered in hardware, software, and firmware, the timely application of corrective actions and/or mitigation steps can reduce the likelihood that adversaries will be able to exploit these vulnerabilities in energy delivery systems. Some of these vulnerabilities may be publicly disclosed before the Supplier can develop remedies; others may be kept from disclosure until remedies are available.

Security breaches may also affect the cybersecurity of the procured product. Such breeches may involve a compromise of security involving the Supplier's organization, or any organization involved in the product's supply chain. Security breaches may result in the loss of sensitive product design

information, information on the Acquirer's use and configuration of the product, a compromise of access control information for the deployed products (e.g., compromise of access control information that the Supplier uses to perform maintenance on a deployed product), or other security-sensitive information. If the Acquirer is informed of a security breach in a timely manner, it may be able to apply mitigating measures to maintain adequate levels of security.

Baseline procurement language:

3.2.1. Upon request of the Acquirer, and prior to the delivery of the procured product, the Supplier shall provide summary documentation of publicly disclosed vulnerabilities in the procured product and the status of the Supplier's disposition of those publicly disclosed vulnerabilities.

3.2.2. The Supplier shall provide, within [a negotiated time period] after product delivery, summary documentation of uncorrected security vulnerabilities in the procured product. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the product. The summary documentation shall include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.

3.2.3. After contract award, the Supplier shall provide summary documentation within [a negotiated time period] of any identified security breaches involving the procured product or its supply chain. Initial and follow-up documentation shall include a description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.

3.3 Problem Reporting

It is difficult to build products that are perfectly secure, and sometimes unknown vulnerabilities exist in the core logic and configuration of energy delivery systems and components. When vulnerabilities in hardware, software, or firmware configurations are discovered by users, a process is needed to allow users to report them. A vulnerability mitigation process allows for the tracking of progress to develop workarounds, patches, and fixes. Timely notification of vulnerabilities is essential to create defenses for zero-day exploits.

Baseline procurement language:

3.3.1. The Supplier shall provide a secure process for users to submit problem reports and remediation requests. This process shall include tracking history and corrective action status reporting.

3.3.2. Upon the Acquirer submitting a problem report to the Supplier, the Supplier shall review the report, develop an initial action plan within [a negotiated time period], and provide status reports of the problem resolution to the Acquirer within [a negotiated time period].

3.3.3. The Supplier shall provide the Acquirer with its responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams [CERTs]), which shall address public disclosure protections implemented by the Supplier.

3.4 Patch Management and Updates

The discovery of product weaknesses and vulnerabilities is an ongoing process for Suppliers. To remediate discovered weaknesses and vulnerabilities, responsible system and product Suppliers regularly release updates, patches, service packages, or other fixes to their products—including third-party hardware, software, and firmware. Testing and validation of the patches and upgrades are necessary prior to performing the updates on a production system.

Baseline procurement language:

3.4.1. The Supplier shall provide documentation of its patch management program and update process (including third-party hardware, software, and firmware). This documentation shall include resources and technical capabilities to sustain this program and process. This includes the Supplier's method or recommendation for how the integrity of the patch is validated by the Acquirer. This documentation shall also include the Supplier's approach and capability to remediate newly reported zero-day vulnerabilities.

3.4.2. The Supplier shall verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to the Acquirer, or within [a pre-negotiated period] after delivery.

3.4.3. For [a negotiated time period of the contract or support agreement], the Supplier shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within [a negotiated time period]. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within [a negotiated time period (e.g., 7, 14, or 21 days)]. If updates cannot be made available by the Supplier within these time periods, the Supplier shall provide mitigations and/or workarounds within [a negotiated time period].

3.4.4. When third-party hardware, software, and firmware is provided by the Supplier to the Acquirer, the Supplier shall provide appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses within [a negotiated time period]. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within [a negotiated time period (e.g., 30, 60, or 90 days)]. If these third-party updates cannot be made available by the Supplier within these time periods, the Supplier shall provide mitigations and/or workarounds within [a negotiated time period].

3.5 Supplier Personnel Management

Supplier personnel who have access to an Acquirer's energy delivery system, or have sensitive information about the system, need to protect this information from adversaries. Without Supplier personnel management processes, sensitive information and access to assets could be compromised when changes to a Supplier's staff occur.

Baseline procurement language for energy delivery systems:

3.5.1. The Supplier shall provide summary documentation to attest to its workforce receiving position-appropriate cybersecurity training and awareness. This includes specialized training for those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of products procured by the Acquirer, as part of the Supplier's cybersecurity program.

3.5.2. The Supplier shall perform security background checks on its employees (including contract personnel) working directly on or involved in the development of an Acquirer's system or procured product. The background check methodology shall be mutually agreed upon by the Acquirer and Supplier.

3.5.3. The Supplier shall ensure that policies and procedures are followed to prohibit the unauthorized disclosure of knowledge, information, architectures, or configuration relevant to the Acquirer's system.

3.5.4. The Supplier shall share information with the Acquirer to support the timely update of authentication credentials and access control to reflect staffing changes.

3.6 Secure Hardware and Software Delivery

Energy delivery systems use information and communication technology (ICT). The modern ICT supply chain is complex and extended, and it provides numerous opportunities for subversion, including malicious code insertion, counterfeit insertion, and tampering. Specifically, ICT, including energy delivery systems, requires protection during delivery, both physical (when components are transported) and logical (when software, including patches, is downloaded). If energy delivery systems and their components are not protected during delivery, the resulting production systems may fail prematurely or exhibit unintended functionality, which can compromise energy delivery system availability, reliability, and integrity.

Baseline procurement language:

3.6.1. The Supplier shall establish, document, and implement risk management practices for ICT supply chain delivery of hardware, software, and firmware. The Supplier shall provide documentation on its:

- Chain-of-custody practices
- Inventory management program (including the location and protection of spare parts)

- Information protection practices
- Integrity management program for components provided by sub-suppliers
- Instructions on how to request replacement parts
- Maintenance commitment to ensure that for a specified time into the future, spare parts shall be made available by the Supplier

3.6.2. The Supplier shall specify how digital delivery for procured products (e.g., software and data) will be validated and monitored to ensure the digital delivery remains as specified. If the Acquirer deems that it is warranted, the Supplier shall apply encryption to protect procured products throughout the delivery process.

3.6.3. The Supplier shall use trusted channels to ship critical energy delivery system hardware, such as U.S. registered mail.

3.6.4. The Supplier shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

3.6.5. The Supplier shall demonstrate chain-of-custody documentation for critical energy delivery system hardware and require tamper-evident packaging for the delivery of this hardware.

4. INTRUSION DETECTION

Intrusion detection is used to detect attempts to compromise the confidentiality, integrity, or availability of energy delivery systems. An intrusion detection system (IDS) is a component, or specialized software residing on a component, that monitors network or system activities for malicious activities or policy violations and logs or reports potential issues. Intrusion detection on energy delivery systems can involve the use of host-based or network-based IDSs.

4.1 Host Intrusion Detection

A host-based intrusion detection system (HIDS) is one of the last layers of protection for the systems on a network. A HIDS is used to monitor and analyze the communication traffic within a system component or energy delivery system. It can also be used to assess communication traffic at the component's network interfaces. The HIDS monitors and reports the configuration of the host system and application activity. A HIDS may perform such functions as log analysis, event correlation, integrity checking, policy enforcement, rootkit detection, performance monitoring, and base-lining to detect variations in system configuration.

Baseline procurement language for the acquisition of a component or energy delivery system with a HIDS:

4.1.1. The Supplier shall provide either a configured HIDS or the information needed for the Acquirer to configure the HIDS.

4.1.2. The Supplier shall implement or recommend a configuration for the HIDS in a manner that adheres to requirements for the Acquirer's operating system functions or business objectives.

4.1.3. The Supplier shall apply the auditing and logging provisions outlined in Section 2.6 of this document to the HIDS.

4.2 Network Intrusion Detection

A network intrusion detection system (NIDS) is used to identify and analyze communication traffic on a computer network and to identify unauthorized or malicious activity. NIDSs can be either knowledge-based or behavior-based. Due to the nature of monitoring, a NIDS generates voluminous logs. If these logs are not properly configured during initial setup, they may become unmanageable, and therefore not useful. Performing the initial configuration of the NIDS is a minor effort compared to the degree of effort required for ongoing log reviews and tuning. Log consolidation, review, and notification software tools should be used to help automate the review of NIDS data.

Baseline procurement language for the acquisition of a component or energy delivery system with a NIDS:

4.2.1. The Supplier shall recommend a placement(s) of the NIDS sensors to provide appropriate monitoring for the energy delivery system network.

4.2.2. The Supplier shall provide traffic profiles with expected communication paths, network traffic, and expected utilization boundaries for behavior-based (also called anomaly based) NIDS.

4.2.3. The Supplier shall provide initial and routinely updated signatures for knowledge-based (also called signature-based) NIDS.

4.2.4. The Supplier shall provide either a configured NIDS or the information needed for the Acquirer to configure the NIDS in adherence to the Acquirer's functional requirements.

4.2.5. The Supplier shall provide a NIDS architecture that works with the system communication method.

5. PHYSICAL SECURITY

Physical security is an important element in cyber defense for energy delivery systems. Physical security is used to deter, delay, detect, and deny physical access by unauthorized individuals, including those who may wish to physically access energy delivery system components in order to compromise the confidentiality, integrity, or availability of the systems or their data. The Acquirer can insert appropriate physical security requests in its procurement language for energy delivery systems.

5.1 Physical Access to Energy Delivery System Components

Physical security is a key aspect of protecting energy delivery systems from manipulation, sabotage, or theft. The innermost level of physical security involves deterring and delaying an adversary from gaining access to the energy delivery system or its components once inside the facility.

Baseline procurement language for the acquisition of new energy delivery systems, when the Acquirer does not have existing physical security enclosures and wishes to include them:

5.1.1. The Supplier shall provide lockable or locking enclosures or rooms for energy delivery systems and system components (e.g., servers, clients, and networking hardware) and for the systems used to manage and control physical access (e.g., servers, lock controllers, and alarm control panels).

5.1.2. The Supplier shall provide a method for tamper detection on lockable or locking enclosures. If a physical security and monitoring system is used, tamper detection shall be compatible.

5.1.3. The Supplier shall change locks, locking codes, keycards, and any other keyed entrances within [a pre-negotiated period] or provide the Acquirer with the tools and instructions for making these changes.

5.1.4. The Supplier shall work with the Acquirer to verify that physical security features do not hamper energy delivery system operations.

5.1.5. The Supplier shall reprogram codes (e.g., remove default codes) on provided locks and locking devices so that the codes/passwords are unique to the Acquirer and do not repeat codes used in the past.

5.1.6. As specified by the Acquirer, the Supplier shall provide two-factor authentication for physical access control.

5.2 Perimeter Access

Perimeter security is one of the first lines of defense for protecting a facility and its internal systems. A breach of this perimeter can lead to the compromise of energy delivery systems. Perimeter security components that restrict physical access to a facility or a portion of a facility include fences, walls, entrance gates or doors, vehicle barriers, surveillance and alarm systems, and security guards.

Perimeter access restrictions are used to prevent unauthorized individuals from entering areas where energy delivery systems and their communication pathways are located.

Baseline procurement language for the acquisition of a physical perimeter access system:

5.2.1. The Supplier shall provide a physical security assessment as specified by the Acquirer and relevant to the procurement that defines the security perimeter physical access points and controls needed at each access point.

5.2.2. The Supplier shall coordinate with local authorities when installing and using remote alarm systems as defined and specified by the Acquirer.

5.2.3. The Supplier shall verify and provide documentation that monitoring and alarm of physical access can be separated from the control network (unless making this communication part of the control network is specifically requested by the Acquirer).

Baseline procurement language when the Supplier is also involved in the operation of the physical perimeter access system:

5.2.4. The Supplier shall allow access within the perimeter only to those employees, contractors, or guests explicitly permitted in such access by both the Supplier and Acquirer.

5.2.5. The Supplier shall verify and provide documentation that security personnel have completed background checks.

5.3 Communications inside the Physical Security Perimeter

Compromise of the communications within a security perimeter can jeopardize the security of energy delivery systems. These communications need to be secured to limit access to energy delivery systems and their data, which should flow to only authorized users. These communications may involve wired or wireless communications.

Baseline procurement language for the acquisition of communications that are internal to the Acquirer's system:

5.3.1. The Supplier shall verify and provide documentation that physical communication channels are secured from physical intrusion.

5.3.2. The Supplier shall verify and provide documentation that communication channels are as direct as possible (e.g., communication paths between devices in the same network security zone do not pass through devices maintained at a lower security level or unnecessarily cross into zones of lower physical security).

6. WIRELESS TECHNOLOGIES

Wireless technologies refer to any technology (e.g., radio, microwave, infrared, and ZigBee) that allows analog and digital communication without the use of wires.

6.1. General Wireless Technology Provisions

Many energy delivery systems and networks use wireless technologies; therefore, it is important to establish and maintain effective and reliable wireless communications links. Unlike wired networks, access to wireless networks does not require physical access or the typical permissions associated with physical access. It is important to utilize sufficient security protections to mitigate the threat of the wireless network being used by individuals without the organization's knowledge or consent.

Baseline procurement language for wireless technology:

6.1.1. The Supplier shall document specific protocols and other detailed information required for wireless devices to communicate with the control network, including other wireless equipment that can communicate with the Supplier-supplied devices.

6.1.2. The Supplier shall document use, capabilities, and limits for the wireless devices.

6.1.3. The Supplier shall document the power and frequency requirements of the wireless devices (e.g., microwave devices meet the frequency requirements of Generic Requirements [GR]-63 Network Equipment Building System [NEBS] and GR-1089).

6.1.4. The Supplier shall document the range of the wireless devices and verify that the range of communications is minimized to both meet the needs of the Acquirer's proposed deployment and reduce the possibility of signal interception from outside the designated security perimeter.

6.1.5. The Supplier shall document that the wireless technology and associated devices comply with standard operational and security requirements specified in applicable wireless standard(s) or specification(s) (e.g., applicable IEEE standards, such as 802.11).

6.1.6. The Supplier shall demonstrate—through providing summary test data—that known attacks (e.g., those documented in the Common Attack Pattern Enumeration and Classification [CAPEC] list, such as malformed packet injection, man-in-the middle attacks, or denial-of-service attacks) do not cause the receiving wireless devices to crash, hang, be compromised, or otherwise malfunction.

6.1.7. The Supplier shall document the configuration control options that enable varying of the security level of the devices.

6.1.8. The Supplier shall allow and recommend alarm settings in accordance with the needs of the system.

7. CRYPTOGRAPHIC SYSTEM MANAGEMENT

A cryptographic-based security system involves both cryptographic methods (e.g., primitives/algorithms) and Cryptographic Key Management (methods of creating, distributing, maintaining, validating, and updating cryptographic keys). This document addresses basic cryptographic system documentation and management capabilities that are to be provided.

This document does not provide requirements related to determining which type of cryptographic-based security system is appropriate for any particular environment; those are critical and complex issues that are beyond the scope of this document. See Federal Information Processing Standard (FIPS) 140-2 and NIST 800-57 for more information on more detailed cryptographic system requirements.

7.1. Cryptographic System Documentation

The strength of cryptographic systems varies widely. Having documentation of how the cryptographic features work and how they should be implemented and managed within a particular environment is critical to the long-term effectiveness of a system. It is important to establish a baseline set of documentation detailing which cryptographic primitives (e.g., algorithms) the Supplier intends to implement in the proposed system, and how those primitives are to be implemented and managed throughout the product life cycle.

Baseline procurement language for cryptographic system documentation:

7.1.1. The Supplier shall document how the cryptographic system protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system as specified by the Acquirer. This documentation shall include, but not be limited to, the following:

- The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm [SHA]-256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the system, and how these methods are to be implemented.
- The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

7.2. Cryptographic Key and Method Establishment, Usage, and Update

Cryptographic systems, once implemented, require the ability to update credentials in an efficient manner. Without these support capabilities, the effectiveness of the overall system will decrease over time. A process of credential updates that requires physically visiting each protected device in a very large, distributed system is unlikely to maintain its effectiveness over time. This section provides requirements for the types of functions that must be provided to enable an Acquirer to effectively manage a large number of devices installed at unattended locations.

Baseline procurement language for cryptographic system establishment, usage, and updates:

7.2.1. The Supplier shall only use “Approved” cryptographic methods as defined in the Federal Information Processing Standard (FIPS) *Security Requirements for Cryptographic Modules* (FIPS 140-2).

7.2.2. The Supplier shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

7.2.3. The Supplier shall ensure that:

- The system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with the *Suggested Cryptoperiods for Key Types* found in Table 1 of NIST 800-57 Part 1.
- The key update method supports remote re-keying of all devices within [a negotiated time period(s)] as part of normal system operations.
- Emergency re-keying of all devices can be remotely performed within [a negotiated time period (e.g., 30 days)].

7.2.4. The Supplier shall provide a method for updating cryptographic primitives or algorithms. (Note: Prior requirements have addressed updating cryptographic keys. This requirement addresses updates to or replacement of the cryptographic method.)

8. REFERENCES

Energy Sector Control Systems Working Group (ESCSWG). *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. ESCSWG, 2011. https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/roadmap.pdf

Exec. Order No. 13,636, "Improving Critical Infrastructure Cybersecurity." 78 Fed. Reg. 11739. February 19, 2013. www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

IEEE. *IEEE 802.11: Wireless LANs*. New York: IEEE. http://standards.ieee.org/about/get/802/802.11.html.

IEEE. *IEEE 802.15: Wireless Personal Area Networks (PANs)*. New York: IEEE. http://standards.ieee.org/about/get/802/802.15.html.

IEEE. *IEEE 802.16: Broadband Wireless Metropolitan Area Networks (MANs)*. New York: IEEE. http://standards.ieee.org/about/get/802/802.16.html.

IEEE. *IEEE 1588 Precision Time Protocol (PTP) Version 2*. New York: IEEE. http://standards.ieee.org/findstds/standard/1588-2008.html.

IEEE. *IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations*. New York: IEEE. http://standards.ieee.org/findstds/standard/1613-2003.html.

International Organization for Standardization (ISO). *ISO/IEC 27036-3:2013 – Information Technology – Security Techniques – Information Security in Supplier Relationships: Part 3 – ICT Supply Chain Security*. Geneva: ISO. www.iso.org/iso/catalogue_detail.htm?csnumber=59688.

International Society of Automation (ISA). *ISA99, Industrial Automation and Control Systems Security*. Research Triangle Park, NC: ISA. www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821.

Internet Engineering Task Force (IETF). "Glossary." IETF. www.ietf.org/glossary.

National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1. Gaithersburg, MD: NIST, 2014. www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

National Institute of Standards and Technology (NIST). *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82. Gaithersburg, MD: NIST, 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

National Institute of Standards and Technology (NIST). *Guidelines for Smart Grid Cybersecurity.* NIST Interagency Report (IR) 7628. Gaithersburg, MD: NIST, 2010. http://csrc.nist.gov/publications/PubsNISTIRs.html

National Institute of Standards and Technology (NIST). *Notional Supply Chain Risk Management Practices for Federal Information Systems*, NISTIR 7622. Gaithersburg, MD: National Institute of Standards and Technology, 2012. http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf.

National Institute of Standards and Technology (NIST). *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 3. Gaithersburg, MD: NIST, 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

National Institute of Standards and Technology (NIST). "Risk Management Framework (RMF) Overview." NIST. http://csrc.nist.gov/groups/SMA/fisma/framework.html. National Institute of Standards and Technology (NIST). *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology, 2013. http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf.

North American Electric Reliability Corporation (NERC). *CIP Standards*. Collection of standards. Atlanta: NERC. www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

Office of Electricity Delivery and Energy Reliability. "Cybersecurity Capability Maturity Model (C2M2) Program." U.S. Department of Energy. http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program.

Office of Electricity Delivery and Energy Reliability. *Electricity Subsector Cybersecurity Risk Management Process*. Washington, DC: U.S. Department of Energy, 2012. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf.

Open Web Application Security Project (OWASP). "OWASP." OWASP. www.owasp.org/index.php/Main_Page.

Software Assurance Forum for Excellence in Code (SAFECode). "About SAFECode." SAFECode. www.safecode.org/about_us.php.

Telcordia Technologies, Inc. *Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment*, GR-1089, Issue 6. Piscataway, NJ: Telcordia Technologies, Inc., 2011. http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=SEARCH&DOCUMENT=GR-1089&.

Telcordia Technologies, Inc. *NEBS Requirements: Physical Protection*, GR-63, Issue 4. Piscataway, NJ: Telcordia Technologies, Inc., 2012. http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=280008510D000537&KEYWORDS=&TITLE=&DOCUMENT=gr-63&DATE=&CLASS=&COUNT=1000&BASICSEARCH=true.

U.S. Department of Defense (DOD). *DoD 5200: DoD Information Security Program*. Washington, DC: DOD, 1997. www.fas.org/irp/doddir/dod/5200-1r/.

U.S. Department of Homeland Security (DHS). *Department of Homeland Security: Cyber Security Procurement Language for Control Systems.* Washington, DC: DHS, 2009. http://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf.

All references accessible as of March 28, 2014.

9. ABBREVIATIONS AND ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
AGA	American Gas Association
APPA	American Public Power Association
BIOS	Basic Input/Output System
C2M2	Cybersecurity Capability Maturity Model
CAPEC	Common Attack Pattern Enumeration and Classification
CEDS	Cybersecurity for Energy Delivery Systems
CERT	Computer Emergency Response Team
CIP	Critical Infrastructure Protection
DCS	Distributed Control System
DHS	U.S. Department of Homeland Security
DMS	Distribution Management System
DMZ	demilitarized zone
DOE	U.S. Department of Energy
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EEI	Edison Electric Institute
EI	Energetics Incorporated
EMS	Energy Management System
EPRI	Electric Power Research Institute
ESCSWG	Energy Sector Control Systems Working Group
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
GR	Generic Requirements
HIDS	host-based intrusion detection system
IA	Information Assurance
ICT	information and communication technology
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IESO	Independent Electric System Operator
IETF	Internet Engineering Task Force
INFOSEC	National Information Systems Security
INL	Idaho National Laboratory
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Organization for Standardization

IT	information technology
LDAP	Lightweight Directory Access Protocol
NEBS	Network Equipment Building System
NERC	North American Electric Reliability Corporation
NIDS	network intrusion detection system
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NTP	Network Time Protocol
OE	Office of Electricity Delivery and Energy Reliability
OT	operations technology
OWASP	Open Web Application Security Project
PNNL	Pacific Northwest National Laboratory
RFI	request for information
RFP	request for proposal
RMP	Electricity Subsector Cybersecurity Risk Management Process
SAFECode	Software Assurance Forum for Excellence in Code
SANS	System Administration, Networking, and Security Institute
SCADA	Supervisory Control and Data Acquisition
SDLC	system development life cycle
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell Terminal Emulation
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UTC	Utilities Telecom Council
VPN	virtual private network
XSS	Cross-Site Scripting

10. GLOSSARY

Acquirers should review sources for common terms and definitions including, but not limited to, the following:

- **IETF Glossary:** www.ietf.org/glossary.html
- **National Information Assurance (IA) Glossary:** www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf
- **National Information Systems Security (INFOSEC) Glossary** (Written by NSA for the National Security Telecommunications and Information Systems Security Committee)**:** www.dtic.mil/docs/citations/ADA433929
- **NERC CIP Standards:** www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- **NERC Glossary of Terms Used in NERC Reliability Standards:** www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf
- **NIST 800-82:** http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
- **NISTIR 7628:** www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

11. ADDITIONAL ACKNOWLEDGEMENTS

In addition to the organizations identified in the Acknowledgements section, the individuals below deserve special recognition for their efforts in producing this document.

Core Writing Team

Nadya Bartol
Utilities Telecom Council

Dave Dunn
Independent Electric System Operator, Ontario

Cliff Glantz
Pacific Northwest National Laboratory

Ed Goff
Duke Energy

Katie Jereza
Energetics Incorporated

Annabelle Lee
Electric Power Research Institute

Rebecca Massello
Energetics Incorporated

Dave Norton
Federal Energy Regulatory Commission

Lori Ross O'Neil
Pacific Northwest National Laboratory

Tom Overman
Electric Power Research Institute

Melanie Seader
Edison Electric Institute

Contributors

Robert Austin
Electric Power Research Institute

Dan Berrett
Idaho National Laboratory

Gary Finco
Idaho National Laboratory

Carol Hawk
U.S. Department of Energy

Diane Hooie
National Energy Technology Laboratory

David Howard
U.S. Department of Energy

Lisa Kaiser
U.S. Department of Homeland Security

Jim Linn
American Gas Association

Galen Rasche
Electric Power Research Institute

Paul Skare
Pacific Northwest National Laboratory

Colleen Winter
Pacific Northwest National Laboratory