Cybersecurity Procurement Language for Energy Delivery Systems

REVIEW DRAFT – February 2014

Energy Sector Control Systems Working Group

Supporting the Electricity Sub-Sector Coordinating Council, Oil and Natural Gas Sector Coordinating Council, and Government Coordinating Council for Energy

Request for Feedback:

Energy sector asset owners, operators, and Suppliers are encouraged to provide feedback and guidance to the Energy Sector Control Systems Working Group (ESCSWG) to enhance the cybersecurity procurement language for future versions of this document. Please send feedback to es-pl@energetics.com.

Disclaimer

Contents

61

62

1.0 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 way of life is made possible by a vast network of processes enabled by these systems as well as the interconnected electronic components, communication devices, and people that monitor and control those processes.

Energy delivery systems are used to monitor and control the production, transfer, and distribution of energy. Two examples of such systems include Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). Energy delivery systems are comprised of the sensors and actuators used for monitoring and controlling, the computer-based systems that analyze and store data, and the communication pathways and networks that interconnect the various computer systems.

Cybersecurity is 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 cyber attack on an energy delivery system can have significant impacts on the availability of the system to perform critical functions, the system integrity, and the confidentiality of sensitive information. Accidental and malevolent cyber threats to energy delivery systems can impact national security, public safety, and the national economy.

Including cybersecurity in the procurement of energy delivery systems is an important step in protecting energy delivery against cyber threats. Including cybersecurity in the procurement process can ensure that suppliers consider cybersecurity starting with the design phase of system development and continuing through the testing, manufacturing, delivery, installation, and product support phases of the product life cycle. This will improve overall reliability and reduce cybersecurity risks over the life of the system. To assist with this process, 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,*[1] which was released in 2009 [henceforth referred

[1] http://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

to as DHS (2009)]. The development of the 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 the U.S. federal and state governments and international stakeholders.

The DHS (2009) document summarizes security principles to consider when designing and procuring control system products and services (software, systems, maintenance, and networks), and provides example language to incorporate 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. The intent was rather to encourage vendors and purchasers 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 taken into account before adding or requesting security features.

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 energy sector 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 (2011)*, developed by the Energy Sector Control Systems Working Group (ESCSWG), provides a common vision and strategic framework for industry and government to design, install, operate, and maintain energy delivery systems that can survive a cyber incident while sustaining the critical energy delivery functions on which the U.S. national security, safety, and economy rely. The Roadmap 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 vision and strategy to build a culture of security, helping to make cybersecurity practices reflexive and expected among energy sector stakeholders.

In addition, the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was designed to improve electricity subsector cybersecurity capabilities and provide a means for utilities 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 public and private sectors. The ES-C2M2 program has produced an evaluation tool to help utilities assess the maturity of their cybersecurity capabilities. Consideration of supply chain issues and cybersecurity procurement are elements in the maturity

model. By including the baseline cybersecurity procurement language identified in this document, utilities can help to further improve their cybersecurity maturity level.

Finally, 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 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.

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 identify the baseline cybersecurity procurement language provided in this document. This language is tailored to the specific needs of the energy sector.

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

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

- Individual components of energy delivery systems (e.g., programmable logic controllers, digital relays, or remote terminal units)
- Individual energy delivery systems (e.g., a Supervisory Control and Data Acquisition system or Distributed Control System)
- Assembled or networked energy delivery systems (e.g., an electrical substation or a natural gas pumping station).

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 Supplier.

Table 1. Definitions for the Different Categories of Procurement Language Users (NIST, 2013).

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, Supplier, or an independent third party. Conversely, Integrators may function as an Acquirer and/or Supplier when developing systems and components for deployment. Therefore, reference to Acquirers and Suppliers in this document pertains to Integrators performing those functions.	NIST IR 7622, adapted

Definitions of specific procurement language terminology included in this document are shown in Table2.

Table 2. Definition of Procurement Language Terminology
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" and "need not" indicate a course of action permissible within the limits of the document.
The term "can" and "cannot" indicate a possibility of something occurring.

Overview of the Document

This document provides baseline cybersecurity procurement language that is the consensus opinion of the document authors and key reviewers from 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 information technology (IT). Considerations for IT cybersecurity are outlined in many standards and guidance documents (e.g., the NIST 800 series of publications). Products and services acquired through the procurement process should comply with the applicable IT security standards as well as those specific to energy delivery systems.

This document aims to cover a broad range of energy delivery system procurements ranging from individual components of systems (e.g., programmable logic controllers (PLCs), human machine interfaces (HMIs), remote terminal units (RTUs), sensors, actuators, and other devices) to complex energy delivery systems (e.g., an electrical substation or a natural gas pumping station). Additionally, this 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., TCP/IP communication between systems or components, remote access capabilities).

Section 2 provides generally applicable cybersecurity considerations that may apply to any type of product being procured for any energy delivery system, except where noted. The language should be tailored by the Acquirer based on the specific product being procured and the environment to 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
- Account Auditing and Logging
- Communication Restrictions
- Malware Detection and Protection
- Heartbeat Signals
- Reliability and Adherence to Standards

Section 3 focuses on the Supplier's product lifecycle security program. The Supplier's product lifecycle security program should cover the design, development, manufacture, storage, delivery of products, implementation, and disposal. If this security program is properly designed and implemented, it 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

Sections 4 provides additional language to consider when acquiring intrusion detection systems; Section 5 focuses on physical security considerations; and Section 6 focuses on wireless technologies.

Section 7 provides some suggested references to review in addition to this document. However, this section does not attempt to list all relevant resources. Section 8 provides a list of acronyms used in this document and Section 9 provides a glossary of some terms that are specific to this document. This document does not attempt to include all common terms and definitions. Acquirers should review documents including, but not limited to, NISTIR 7628, NIST 800-82, IEC 62443, NERC Critical Infrastructure Protection Standards (CIPS) for common terms and definitions.

1.5 How to Use This Document

This document is intended for use by:

- 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 (RFP) or requests for information (RFI).
- Acquirers seeking to evaluate the cybersecurity maturity of energy delivery system(s) or components offered by Suppliers and Integrators.
- Suppliers and Integrators designing 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 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.

A summary of key points on how to use this document are included below in Figure 1. 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 cyber security-related procurement language in this document is intended for use by Acquirers, Integrates, and Suppliers.
- The procurement language presented in this document is *not* intended to be inserted 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 RFI. Additionally, Suppliers may also go beyond this baseline when proposing products or services in response to an RFP or RFI.

Modifying Procurement Language:

- Cybersecurity procurement language may be modified as agreed upon by the Acquirer and Supplier to meet the specific procurement.
- Procurement language should only be included in contracts if it provides value. If the Acquirer and Supplier agree that a specific element of the language does not add value it may be dropped or be 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 and 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 integration of those components.

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 RFI. Acquirers should review other resources provided by entities including, but not limited to, NIST, NERC, SANS (less commonly known as the System Administration, Networking, and Security

Institute), International Society of Automation (ISA), International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC) that may provide additional information or cybersecurity language pertaining to a specific procurement. There are also some explicit, mandatory compliance standards (e.g., NERC CIPs) that should be evaluated by Acquirers. 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 7).

Suppliers may also go beyond this baseline cybersecurity procurement language when proposing products or services in response to an RFP or 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 vary and 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. Acquires and Suppliers 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 provides value. If the Acquirer and Supplier agree that a specific element of the language 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 to guard against any inadvertent impacts on required safety features or essential functionality of the energy delivery system or component.

It is recommended that 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. Acquirers 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 meets 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 be discretionary and can be negotiated.

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 Integrator, and adjust their contract language as appropriate for each. In some cases, specific language may apply to both Suppliers and Integrators.

Additionally, Acquirers should consider cybersecurity implications when an energy delivery system has components acquired from multiple Suppliers. Maintaining appropriate cybersecurity in such a system may require additional language that ensures the secure integration of components from multiple Suppliers.

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.

Un-applicable 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 states:

> *2.4.3 The Supplier shall not, unless specifically requested by the Acquirer, allow multiple concurrent logins using the same authentication credentials, 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 multiple concurrent logins are needed using the same authentication credentials on the procured product to support its intended operation, the Acquirer and Supplier can make an exception to this item and permit this capability. To compensate for allowing this, the Acquirer may wish to implement compensating security controls (e.g., enhanced physical security or the disabling of remote access) as part of the procurement or as a separate activity. The decision to drop this procurement language should be documented by the Acquirer and incorporated as a record in their security risk management system. In addition, a description of any compensating security controls that offset the risks associated with dropping of this procurement language should also be documented.

Another example of procurement language that the Acquirer and Supplier may mutually agree is not applicable for 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 situations where procurements that include 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 decision to drop this language should be documented by the Acquirer and incorporated as a record in their security risk management system. If alternative security controls are adopted instead, these also should be documented.

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 3 in Section 3.3 states:

3.3.3 Post-contract award, upon the Acquirer submitting a problem report to the Supplier, the Supplier shall review the report and develop an initial action plan within [negotiated time period].

Acquirers should fill in the time period requested within the brackets before issuing an RFP or RFI. This time period should be tailored to 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

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

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

Acquirers may wish to request additional or more detailed documentation if that is what is needed to ensure their cybersecurity expectations are met.

Some procurement language requesting documentation or summary documentation may drift into areas that involve sensitive information that the Supplier does not wish to fully disclose to their customers or the public. For example, Item 3 in Section 2.7 states:

444 *2.7.3 The Supplier shall provide a method to restrict communications traffic between*
445 *different network security zones. The Supplier shall provide documentation on any*
446 *method or equipment used to restrict communication traffic.*
447
448 This procurement language is not intended to require that the Supplier provide sensitive information
449 to the Acquirer. If the Supplier determines that the information that may be requested is sensitive, the
450 Acquirer and Supplier will need to negotiate how to proceed. An agreement may be reached that the
451 information provided to the Acquirer will be "sanitized" to meet the Acquirer's information needs and
452 the Suppliers need to protect their sensitive information. Alternatively, the Supplier can propose
453 procurement language stating that the Acquirer will need to maintain an appropriate information
454 security program that securely maintains any sensitive information provided to the Acquirer.
455
456

2.0 GENERAL PROCUREMENT LANGUAGE

This section presents cybersecurity-based procurement language that may be generally applicable to energy delivery system procurements, whether a single component, a complete energy delivery system, or a set of integrated energy delivery systems. Prior to using this language for procurement contracts, it should be tailored to a single component, a complete system, or an 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 that are left enabled are possible 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 vulnerabilities in these services leading to the compromise of the energy delivery system. These vulnerabilities can be addressed in a variety of ways. For example, disabling ports and services or removing applications that are not needed for energy delivery systems operation and maintenance. This concept is captured in 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. 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 except for those dedicated to software development
- 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

- Sample programs and scripts

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 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). The Supplier shall provide documentation that identifies all of the unneeded ports, connectors, and interfaces and how they have been disabled.

2.1.4. The Supplier shall configure the system 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 normal computer authentication in the procured product, often referred to as backdoors, and provide written documentation that all such backdoors created by Supplier developers have been permanently deleted from the system.

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

2.2 Access Control

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 to which they are authorized and that are necessary for operation. 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 by individual identities.

Baseline procurement language:

2.2.1. The Supplier shall configure each component 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 for 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 system such that when a session or interprocess communication is initiated from a less privileged application, access control shall be enforced at the most privileged 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 inform the customer how to set a Basic Input/Output System (BIOS) password to protect the BIOS from unauthorized changes. 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 measures.

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

2.2.9. The Supplier shall deliver a system that enables the ability to configure its components to limit access to and from specific locations on the network to which the components are attached, where appropriate, and provide documentation of the system's configuration as delivered.

2.3 Account Management

Many energy delivery systems are configured with default accounts with 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 accounts (including default) that need to be active for proper operation of the energy delivery system.

2.3.2. The Supplier shall change default account settings to Acquirer-specific settings. The Supplier shall not publish changed account information. The Supplier shall provide new account information to the Acquirer via protected mechanism.

2.3.3. Prior to delivery of the procured product to the Acquirer, the Supplier shall disable, remove, or modify any accounts that are not needed for proper operation or maintenance of the energy delivery system. Accounts that are modified 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 or components. 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., Secure Sockets Layer [SSL], tunneling through Secure Shell Terminal Emulation [SSH], Transport Layer Security [TLS]).

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

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.

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

2.5 Authentication/Password Policy and Management

The need for instant 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.

2.5.2. The Supplier shall provide a configurable account password management system that allows for 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, and 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 (e.g., be compatible with) the Acquirer's implementation of multi-factor 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 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, and documentation showing equivalent results in running validation tests against the direct login and the single-sign-on.

2.6 Account Auditing and Logging

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 cyber attacks in time to take protective actions, perform diagnostics, and carry out forensics activities in the event of a successful cyber attack. 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 a system that provides logging capabilities that can be configured by the Acquirer and support the Acquirer's security auditing requirements.

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

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

2.6.4. The Supplier shall ensure logging does not adversely impact system performance requirements.

2.6.5. The Supplier shall implement an approach for collecting and storing (e.g., transfer, log forwarding) security log files that protect the confidentiality and integrity of the logs.

2.6.6. The Supplier shall recommend log management and Security Information and Event Management (SIEM) tools and/or integration with existing tools (e.g., syslog).

2.7 Communication Restrictions

Networks can be partitioned into multiple segments to enhance security by placing technical security controls (e.g., firewalls, unidirectional communication devices, or virtual private network (VPN) concentrators) between the network segments. Hardware and software 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. Poorly designed network architectures are vulnerable to cyber exploitation.

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 their energy delivery system.

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 initiating communication.

2.7.3. The Supplier shall provide a method to restrict communications 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 subnets 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 situations. If the Acquirer has the responsibility of procuring their own firewalls, the Supplier shall recommend appropriate firewall rule sets or rule set guidance for normal and emergency situations. 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 administrative access to network components, 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 delivered systems use unique routable network addresses (e.g., do not use 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8) 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 superior form of security isolation), for the communications tunneling server to reside.

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 (e.g. connectors, filters, concentrators) to provide endpoint to endpoint protection 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 and changing 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, network tap).

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 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 much more susceptible to malware infections and require cyber protections.

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 system 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 and provide an updating scheme for malware signatures. The Supplier shall also test major updates to malware detection applications

- 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 defined 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 cybersecurity services running on the procured product (e.g., virus checking, 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 or software to indicate normal operation or to synchronize with other components within an energy delivery system. If a heartbeat signal is not received in the prescribed time, this is an indication that the component generating the signal is not operating within its normal parameters. Heartbeat status signals can be sent over serial connections or routed protocols. Heartbeat signals can be configured in the hardware, software, or firmware. Problems may arise when heartbeat signals or protocols are corrupted, spoofed, or possibly used as an entry point for unauthorized access.

Baseline procurement languages:

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. Post-contract award, 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

Security standards should be considered when procuring energy delivery systems or their components in order to support 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.

822
823 2.10.2. The Supplier shall verify that the addition of security features does not adversely
824 affect connectivity, latency, bandwidth, response time, and throughput specified.
825
826 2.10.3. The Supplier shall use an implementation that complies with the current applicable
827 interoperability and security standards, as specified by the Acquirer (e.g., ISA 99, IEEE
828 1613, IEEE 1588, NERC CIP).
829
830 2.10.4. Post-contract award and upon Acquirers request, the Supplier shall return or
831 document the secure disposal of Acquirer's data and Acquirer-owned hardware that is
832 no longer needed by the Supplier (e.g., NIST SP 800-80).
833

3.0 THE SUPPLIERS LIFECYCLE SECURITY PROGRAM

The Supplier's lifecycle security program is an important consideration in the procurement process. Vulnerabilities frequently result from architecture, design, and weaknesses and vulnerabilities in software and hardware coding. Many energy delivery system security vulnerabilities are the direct result of writing software with inadequate attention to defense against deliberate and persistent malicious attack. Lifecycle security programs provide a structured way for developing robust products with fewer weakness and vulnerabilities or finding and remediating them before software and systems are delivered and installed in the Acquirer 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 or software 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 lifecycle (SDLC). These practices help to develop hardware, firmware, and software with fewer weaknesses and vulnerabilities, and identify and remediate them 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. Pre-contract award, the Supplier shall provide summary documentation of its secure development lifecycle including 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, firmware, and software. If applicable, the Supplier shall document how the most critical Web application security weaknesses (e.g., as outlined *in OWASP Top 10 or SANS Top 25 Most Dangerous Software Errors*) are addressed in the Supplier's SDLC.

3.1.2. The Supplier shall demonstrate that hardware, firmware, and software are appropriately protected prior to being delivered to the Acquirer. *For example, for software this might include secure code repositories, traceability of who made what changes to code, and other measures.*

3.1.3. The Supplier shall validate that software and firmware have been implemented as required using defined validation tests such as fuzz testing, static testing, dynamic testing, and penetration testing to identify and address weaknesses and

vulnerabilities; use positive and appropriate negative tests to verify that the system or element operates in accordance with requirements and without extra functionality; and monitor for unexpected or undesirable behavior during test. This may be done by an independent entity.

3.1.4. Post-contract award, the Supplier shall provide summary documentation of its coding reviews and security testing, including 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., company support email address, company support phone number), identified by the Acquirer. The Supplier shall communicate with the Acquirer within [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 (RFI), Cross-Site Scripting (XSS), and buffer overflow.

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

3.1.8. The Supplier shall conduct an independent security review of the procured product as delivered and provide a summary of that report to the Acquirer. This may be conducted by the Supplier or third-party.

3.2 Documentation and Tracking of Vulnerabilities

When vulnerabilities are discovered in deployed energy delivery system software, hardware, and system architectures, appropriate documentation and mitigation steps should be taken in a timely fashion to reduce the chances of adversaries exploiting them to access systems. Guidance from Suppliers about vulnerabilities, corrective actions, fixes, or monitoring is needed to reduce potential impacts. Large software Suppliers practice responsible vulnerability disclosure practices, which include collaborating with Acquirers before releasing the information regarding vulnerabilities to the public. Vulnerabilities are normally closely held until recommended mitigations become available. However, some vulnerabilities are made public by those who discover them before a fix has been developed.

Baseline procurement language:

3.2.1. The Supplier shall provide summary documentation of steps for mitigating vulnerabilities.

3.2.2. Upon request of the Acquirer, the Supplier shall provide summary documentation of publically disclosed vulnerabilities in procured products and services prior to delivery to the Acquirer, as well as disposition status.

3.2.3. Post-contract award, the Supplier shall inform the Acquirer in writing of problem reports, vulnerabilities, or security breaches that may affect the security of the Acquirer's procured product or service, regardless of origin of discovery of the problem, in [negotiated time period]. Initial and follow-up notifications shall include, but is not limited to, documentation describing the vulnerability, its potential security impact, root cause, and corrective actions.

3.3 Problem Reporting

Vulnerabilities exist in core logic and configuration of energy delivery systems. When vulnerabilities in software or hardware configuration 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. The process shall include tracking history and corrective action status reporting.

3.3.2. Post-contract award, the Supplier shall provide summary documentation of identified and uncorrected security vulnerabilities in their products and services prior to delivery to the Acquirer. These vulnerabilities shall be addressed by the Supplier by recommending compensating technical security controls and/or by providing mitigations and/or procedural workarounds prior to delivery to the Acquirer, or within a pre-negotiated period after delivery.

3.3.3. Post-contract award, upon the Acquirer submitting a problem report to the Supplier, the Supplier shall review the report and develop an initial action plan within [a negotiated time period].

3.3.4. The Supplier shall provide the Acquirer with their responsible disclosure and threat reporting policies and procedures (e.g. CERTs), which shall address public disclosure protections implemented by the Supplier.

3.4 Patch Management and Updates

Responsible system and product Suppliers regularly release updates, patches, service packages, or other fixes to their products to address known and potential vulnerabilities. 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. Pre-contract award, the Supplier shall provide documentation of its patch management and update process.

3.4.2. The Supplier shall verify and provide documentation that procured products 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. Post-contract award for [negotiated time period of the contract or support agreement], the Supplier shall provide appropriate software updates to mitigate newly discovered vulnerabilities or weaknesses within a [negotiated time period]. For example, critical vulnerabilities are mitigated within a certain number of [7, 14, 21] days. If updates cannot be made available within this time, Supplier shall provide mitigations and/or workarounds within [negotiated time period]. The Supplier shall apply, test, and validate the appropriate updates and/or workarounds before delivery.

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 could be compromised when changes to Suppliers 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. This includes specialized training for those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of products procured by the Acquirer.

3.5.2. The Supplier shall perform security background checks on their employees (including contract personnel) working directly on an Acquirer system.

3.5.3. Pre-contract award, the Supplier shall ensure that policies and procedures are in place to prohibit the unauthorized disclosure of knowledge relevant to the Acquirers system that could lead to a reduction in security.

3.5.4. The Supplier and Acquirer shall share information to support the timely update of authentication credentials 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 provides numerous opportunities for subversion including malicious code insertion, counterfeits 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 and software. 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, 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 delivery process.

3.6.3. The Supplier shall use trusted channels to ship critical energy delivery system components, 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 components and require tamper-evident packaging for the delivery of these components.

4.0 INTRUSION DETECTION

Intrusion detection is "the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource". 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 used to monitor and analyze the communication traffic within a component or energy delivery system. It can also be used to assess communications traffic at the component's network interfaces. The HIDS monitors and reports on 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 does not negatively impact the host'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 identify unauthorized or malicious activity. There are two approaches used by NIDS, knowledge-based and 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 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. Pre-contract award, the Supplier shall provide a recommended placement of the NIDS 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. Post-contract award, the Supplier shall provide either a configured NIDS or provide the information needed for the Acquirer to configure the NIDS.

4.2.5. The Supplier shall provide a network intrusion protection system architecture that shall work 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 control system components in order to compromise the confidentiality, integrity, or availability of energy delivery systems or their data. The Acquirer can insert appropriate physical security requests in their procurement language for energy delivery systems.

5.1 Physical Access to Energy Delivery System Components

Physical security must be taken into account to protect 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 system components (e.g., servers, clients, and networking hardware) and the systems used to manage and control physical access (e.g. servers, lock controllers, 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 according to 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. If required by the Acquirer, the Supplier shall provide two-factor authentication for physical access control.

5.2 Perimeter Access

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, if required 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 requested 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 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

Communications within a security perimeter need to be secured to limit access to energy delivery systems and their data flows to authorized users. These communications may involve wired or wireless communications.

Baseline procurement language for the acquisition of communications that are internal to the Acquirers 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, ZigBee) which allows analog and digital communication without the use of wires.

6.1. General Wireless Technology Provisions

Unlike wired networks, access to wireless networks does not require physical access or the typical permissions associated with physical access, but simply being able to detect and join the network. It is important to utilize sufficient security protections to mitigate the threat of the wireless network being used by any individuals without the organization's knowledge or consent to do so.

Baseline procurement language for wireless technology:

6.1.1. The Supplier shall document specific protocols and other detailed information required for the wireless device 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. *For example, microwave devices shall meet the frequency requirements of GR-63 NEBS and GR-1089 (or their successor requirements).*

6.1.4. The Supplier shall document the range of the wireless devices and verify that this range of the wireless 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 provide the wireless devices with security features, such as passwords or security codes, and encryption or other appropriate technologies to

protect the device from unauthorized access, disclosure, modification, or use. The Supplier shall clearly identify these security features and change them from the Supplier-configured or manufacture default conditions.

6.1.7. 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 device to crash, hang, or otherwise malfunction.

6.1.8. The Supplier shall document the configuration control options that enable varying of the security level of the device.

6.1.9. The Supplier shall allow and recommend alarm settings in accordance to the needs of the system.

7. REFERENCES

DoD 5200 DoD Information Security Program

GR-63 NEBS (Network Equipment-Building System) Requirements: Physical Protection

GR-1089 Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment

IEEE 802.11 Wireless LANs

IEEE 802.15 Wireless Personal Area Networks (PANs)

IEEE 802.16 Broadband Wireless Metropolitan Area Networks (MANs)

IEEE 1588 Precision Time Protocol (PTP) Version 2

IEEE 1613 IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations

ISA SP99 Industrial Automation and Control Systems Security

ISO/IEC 27036-3:2013 – Information Technology – Security Techniques – Information Security in Supplier Relationships: Part 3 – ICT Supply Chain Security

NERC CIP (Critical Infrastructure Protection) standards

NIST SP 800-161, 2013 NIST Supply Chain Risk Management

NIST IR 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems

Open Web Application Security Project (OWASP)

SAFECode Software Assurance Forum for Excellence in Code

All references accessible as of November 1, 2013.

8. ACRONYMS

Acronym	What it Stands For…
BIOS	Basic Input/Output System
CAPEC	Common Attack Pattern Enumeration and Classification
CIPAC	Coordinating Council for Energy under the Critical Infrastructure Partnership Advisory Council
CIPS	Critical Infrastructure Protection Standards
DHS	Department of Homeland Security
DMZ	demilitarized zone
DOE	U.S. Department of Energy
ESCSWG	Energy Sector Control Systems Working Group
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
FAT	Factory Acceptance Test
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HMI	Human Machine Interface
ICT	information and communication technology
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers=
INL	Idaho National Laboratory
ISA	International Society of Automation
ISO	International Standards Organization
MAC	media access control=
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OE	Office of Electricity Delivery and Energy Reliability
OSWAP	Open Web Application Security Project
PAN	personal area network
PNNL	Pacific Northwest National Laboratory
RFI	Remote File Include
RMP	Electricity Subsector Cybersecurity Risk Management Process
RTU	Remote Terminal Unit
SAFECode	Software Assurance Forum for Excellence in Code
SANS	System Administration, Networking, and Security Institute
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SDLC	Software Development Lifecycle

SIEM	Security Information and Event Management
SQL	Structured Query Language
SSH	Secure Shell Terminal Emulation
SSL	Secure Sockets Layer
SSO	Single Sign-On
TCP/IP	Transmission Control Protocol/ Internet Protocol
VPN	Virtual Private Network
WMN	Wireless Mesh Networks
XSS	Cross-Site Scripting

9. GLOSSARY

Access control—The management of admission to system and network resources. It grants authenticated users access to specific resources based on company policies and the permission level assigned to the user or user group. Access control often includes authentication, which proves the identity of the user or client machine attempting to log in.

Access Control List (ACL)—A table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its ACLs. The list has an entry for each system user with access privileges.

Authentication—The process of verifying an identity claimed by or for a system entity. Also, any security measure designed to establish the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information. Authentication is generally associated with a password and/or token(s) entered into a host system for gaining access to computer application(s) by a computer user. For example, the authentication may examine "what you have" (e.g., a key), "what you know" (e.g., username and password), and "what you are" (e.g., biometric scan).

Backdoor—A hidden method for bypassing normal computer authentication.

BIOS— Basic Input/Output System. BIOS refers to the software code run by a computer when first powered on. The primary function of BIOS is to prepare the machine so other software programs stored on various media (such as hard drives, floppies, and CDs) can load, execute, and assume control of the computer. This process is known as booting up.

Client—A user's computer which relies on another computer, usually referred to as the server, to provide or serve resources. This relationship centralizes resources and reduces service redundancy.

Control System (CS)—An interconnection of components (computers, sensors, actuators, communication pathways, etc.) connected or related in such a manner to command, direct, or regulate itself or another system, such as chemical process plant equipment/system, oil refinery equipment/systems, electric generation/distribution equipment/systems, water/waste water systems, manufacturing control systems, etc.

Cross-Site Scripting (XSS) —Are a type of problem in which malicious scripts are injected into the otherwise benign and trusted Web sites.

Encryption—In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge.

Factory Acceptance Test (FAT) —A test conducted at the Vendor's premise usually by a third party to verify operability of a system according to specifications.

Firewall—Hardware and/or software that functions in a networked environment to prevent some communications forbidden by the security policy. It has the basic task of controlling traffic between

different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with higher trust).

Firmware—Software that is embedded in a hardware component. It is often provided on flash ROMs or as a binary image file that can be uploaded onto existing hardware by a user.

Heartbeat Signals—Also known as a watchdog timer, keep-alive, or health status. The signals indicate the communications health of the system.

Human-Machine Interface (HMI)—Refers to the layer that separates a human that is operating a machine from the machine itself. One example of a human-machine interface is the computer hardware and software that enables a single operator to monitor and control large machinery remotely.

Host-based Intrusion Detection System (HIDS)—An application that detects possible malicious activity on a host from characteristics such as change of files (file system integrity checker), operating system call profiles, etc.

Intrusion Detection System (IDS)—Software or an appliance used to detect unauthorized access or malicious or abnormal operation to a computer system or network. IDS systems that operate on a host to detect malicious activity are called host-based IDS systems or HIDS. IDS systems that operate on network data flows are called network-based IDS systems or NIDS.

Internet Protocol (IP)—A data-oriented protocol used by source and destination hosts for communicating data across a packet-switched internetwork. Data in an IP internetwork are sent in blocks referred to as packets or datagrams (these terms are basically synonymous in IP).

Internet Protocol Versions 4 (IP) and 6 (IPv6) —Specify the format of packets and the addressing scheme used to communicate using TCP/IP. Version 4 (IPv4) uses a 32-bit addressing scheme, while its successor, Version 6 (IPv6), provides a number of improvements including the expanded capability of a 128-bit addressing scheme.

Malware—Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, rootkits, spyware, and adware.

Network Intrusion Detection System (NIDS)—A hardware tool that monitors IP traffic on a network segment (or segments) to detect unauthorized access to a computer system or network.

Packet—A structured and defined part of a message transmitted over a network.

Patch—A fix for a software program where the actual binary executable and related files are modified.

Post-contract Award—A term meaning a point in time in which all terms of the contract have been agreed. Some sensitive information need not be shared during the bidding process but does when the contract is awarded. The term would be used in a procurement specification to indicate expectations upon the Vendor by the Purchaser for information of products necessary after the contract is awarded.

Principle of Least privilege—The security objective of granting users only those accesses they need to perform their official duties.

Programmable Logic Controller (PLC)—A programmable microprocessor-based component designed to control and monitor various inputs and outputs used to automate industrial processes.

Port (network)—An interface for communicating with a computer program over a network.

Port mirroring—Also known as a roving analysis port, is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack.

Rootkits—Sets of programs that are introduced into a computer system without permission of the computer operator to obtain privileged access, which would allow control of the computer, usually with capabilities to avoid detection.

Scanning—Can refer to any of the following:

- Active Port Scanning—Actively sending out network packets to enumerate all the open ports of a component, including both TCP and UDP Port ranges 0–65535.
- Passive Traffic Mapping/Scanning—Passively recording network traffic, usually through the use of span/monitor ports on the networking hardware. This discovers the ports that are normally used, but will not detect open ports that are not actively used by the system. As such, this method will provide an incomplete view of what services/ports are available.
- Security Scanning—A nebulous term that could refer to any type of scanning.
- Version Scanning—Actively attempts to discover the protocol and the protocol version by connecting to the open ports and performing a sequence of fingerprinting actions.
- Vulnerability Scanning—Actively connects to the remote device and attempts to exploit known vulnerabilities. Often includes active port scanning and version scanning to first discover the vulnerabilities.

Role-based access controls (RBAC)—Refers to limiting 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 which they are entitled to and that are necessary for operation.

Supervisory Control and Data Acquisition (SCADA)—A SCADA computer system is developed for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation.

Security breaches—Refers to unauthorized access to data or computing resources that compromises the availability, confidentiality, or integrity of the system.

Server—A computer or component on a network that manages network resources. For example, a file server is a computer and storage component dedicated to storing files, a Web server for access to Web content, a DNS server for domain name services, a database server for access to relational tables, an email server for access to email, etc.

Services—Software application that facilitates communications to other applications or components either local or distributed. Services are typically associated to a port. Sometimes services are referred to as software ports.

Single Sign-on—A specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems normally enabled by role-based access control.

Site Acceptance Test (SAT)—A test conducted at the customer location, often by a third party, to verify operability of a system according to specifications immediately prior to commissioning.

Supply Chain—NIST SP 800-161 defines ICT supply chain as a linked set of resources and processes between Acquirers, Integrators, and Suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling and delivery of ICT products and services to the acquirer.

Transmission Control Protocol (TCP)—One of the main protocols in TCP/IP networks. Whereas, the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data over many packets. TCP includes mechanisms and protocols to ensure delivery of the data in the correct sequence from source to destination.

Upgrade—Generally, an upgrade is a new release of software, hardware, and/or firmware replacing the original components to fix errors and/or vulnerabilities in software and/or provide additional functionality and/or improve performance.

Validate—The process of evaluating a system during or at the end of the development process to determine whether it satisfies specified business requirements.

Virtual Private Network (VPN)—A private, encrypted communications network usually used within a company, or by several different companies or organizations, used for communicating in a software tunnel over a public network.

Workstation—A workstation is a computer designed for professional use by a single user.

Worm—A computer worm is a self-replicating computer program similar to a computer virus. In general, worms harm the network and consume bandwidth.

ZigBee—A specification for a suite of high-level communication protocols used to create PANs built from small, low-power digital radios. Though low-powered, ZigBee devices often transmit data over longer distances by passing data through intermediate devices to reach more distant ones, creating a mesh network; i.e., a network with no centralized control or high-power transmitter/receiver able to reach all of the networked components. ZigBee is based on an IEEE 802.15 standard.

Wired Mesh Networks (WMNs)—Consist of the end devices or end nodes that could be a sensor or other asset. These assets are connected to the mesh network via a wireless router or repeater unit that is used to forward its data to the central host. It can be implemented with various wireless technologies including the IEEE 802.11, 802.15, and 802.16 standards.

WiMAX (Worldwide Interoperability for Microwave Access)—A wireless communication standard that is designed to provide final long-distance wireless connectivity. It is covered by the IEEE 802.16 standard (http://en.wikipedia.org/wiki/WiMAX).