PNNL- 28661

Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities

May 2019

Michael Mylrea, JA Rotondo, Sri Nikhil Gupta Gourisetti

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL- 28661

Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities

May 2019

Michael Mylrea, JA Rotondo, Sri Nikhil Gupta Gourisetti

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

This document provides a short overview of cybersecurity procurement and implementation guidelines for federal facilities to complement the Task Order Request for Proposal (TO RFP) used by an ordering agency to communicate agency-, site-, and project-specific terms and conditions.

Acronyms and Abbreviations

AMI	Advanced Metering Infrastructure
BAS	Building Automation Systems
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
EO	Executive Order
EERE	Office of Energy Efficiency and Renewable Energy
FEMP	Federal Energy Management Program
ICS	Industrial Control Systems
IDIQ	Indefinite Delivery, Indefinite Quantity
IT	Information Technology
SCADA	Supervisory Control and Data Acquisition
TO RFP	Task Order Request for Proposal

Contents

Summary ii
Acronyms and Abbreviations........ iii
Contents iv
1.0 Introduction 1
1.1 Background........ 1
1.2 How to Use This Document 1
1.2.1 Terminology........ 2
2.0 Key Procurement Recommendations 3
2.1 Lifecycle Cybersecurity 3
2.2 Additional Considerations for Federal Facilities........ 4
2.3 General Cybersecurity Procurement Considerations........ 5
3.0 Elements of a Cybersecurity Procurement Plan........ 6
3.1 Cybersecurity Assessment Process Considerations 6
4.0 References........ 7

Figures

Figure 1: Cybersecurity Procurement Lifecycle 4

Tables

Table 1. Definitions for the Different Categories of Procurement Language Users........ 2

1.0 Introduction

The following is a short overview of cybersecurity procurement and implementation guidelines for federal facilities to complement the Task Order Request for Proposal (TO RFP) used by an ordering agency to communicate agency-, site-, and project-specific terms and conditions.

1.1 Background

The Department of Homeland Security (DHS) has warned of increasing cyberattacks targeting energy technologies and associated industrial control systems (ICS), which are essential to the operations of technology and systems across federal facilities. A cyberattack on energy technologies can have significant impacts on the availability of a system or asset to perform critical functions as well as the integrity of the system and the confidentiality of sensitive information. White House Executive Order (EO) 13800 directs federal agencies to support cyber risk management efforts for critical infrastructure, and to work with the energy sector to identify, protect, detect, respond, and recover from cyberattacks targeting energy infrastructure.

While critical cyber assets such as supervisory control and data acquisition (SCADA) systems, building automation systems (BAS), advanced metering infrastructure (AMI), and ICS found in critical energy infrastructure can have unique software, firmware, application, vendor, and communications protocols, the procurement requirements to insure the confidentially, integrity, authentication and availability share a number of similarities.

Embedding cybersecurity in the procurement of energy technologies used in federal facilities is an important step for protecting these assets, systems, and sites and is the focus of this document. Including cybersecurity in the procurement process helps to ensure that those purchasing and supplying energy technologies consider cybersecurity from the design phase (see Figure 1), which ensures cybersecurity is implemented throughout the procurement lifecycle. Leveraging and adapting the following draft cybersecurity procurement and implementation language may provide an immediate and timely opportunity to expand and solidify cybersecurity procurement language with new and existing vendors of critical cyber assets.

Implementing cybersecurity procurement and implementation guidelines would help mitigate systems level and supply chain cyber threats, expediting secure and sustainable deployment and integration of critical SCADA, smart systems and automation technology.

1.2 How to Use This Document

This document is tailored to the specific needs of federal facilities to provide a ***starting point*** for federal facility energy cybersecurity procurement. However, as the cybersecurity landscape continues to evolve, new threats, technologies, techniques, practices, and requirements may need to be considered during the procurement process.

This document does not attempt to specify or replace cybersecurity-based procurement language for acquisitions involving information technology (IT), as considerations for IT cybersecurity are outlined in many standards and guidance documents. Users of this document have the responsibility of ensuring that actions taken during the procurement process comply with current standards and regulations.

Language listed in the Key Procurement Recommendations section is not intended to be directly inserted (or attached) into a procurement contract; best practice dictates that specific language, appropriate for the applicable procurements, should be negotiated based on the system, component, or service and the intended application of the energy technology in accordance with cybersecurity risk tolerance or agency guidelines. Specific procurement language should be agreed upon by both the Acquirer's and Supplier's contracting offices.

1.2.1 Terminology

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.[1]

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

Procurement Language User	***Definition***
Acquirer	Stakeholder that acquires or procures a product or service.
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.
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.

[1] Energy Sector Control Systems Working Group (ESCSWG) (April 2014). "Cybersecurity Procurement Language for Energy Delivery Systems."

2.0 Key Procurement Recommendations

The below recommendations are not intended to be directly inserted (or attached) into a procurement contract, but rather as a starting point to be tailored as necessary based on the system, component, or service and the intended application of the energy technology in accordance with cybersecurity risk tolerance or agency guidelines.

- 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.
- 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].
- 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.
- 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.
- 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.
- 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.
- 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.

2.1 Lifecycle Cybersecurity

Cybersecurity procurement language should consider cybersecurity procurement lifecycle, including product design, development, manufacturing, storage, delivery, implementation, maintenance, and disposal. Considerations of lifecycle security programs can result in the installation of products with fewer weaknesses and vulnerabilities or finding and remediating them before software and systems are delivered and installed in the Acquirer's environment.

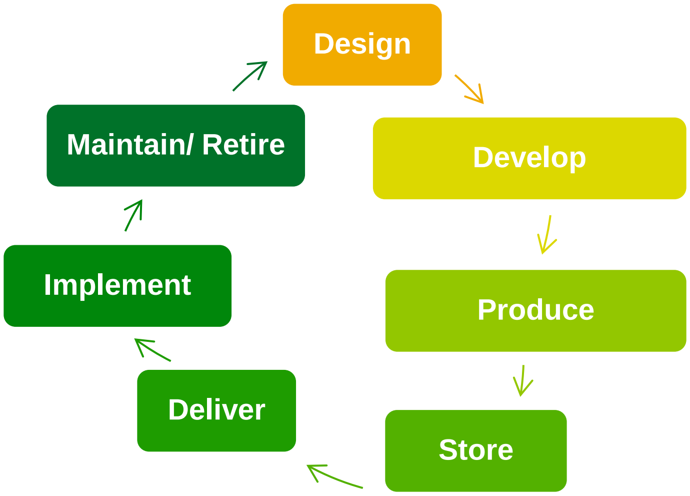

Figure 1: Cybersecurity Procurement Lifecycle

Agencies should consider supplier lifecycle cybersecurity programs in the procurement process that include:

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

2.2 Additional Considerations for Federal Facilities

Federal facilities may also choose to include language from the below list in procurement language and/or service-level agreements:

- **Timely notification** of vulnerabilities or breaches, with accompanying mitigating measures (testing/validation of patches and updates): Require vendors to patch and or update critical systems when a breach is reported or discovered
- **Supply chain security**: Require vendors to demonstrate they have significant supply chain security:
  - Secure cloud, supply chain, secure code development
  - Minimal cyber requirements in design and implementation stage
- **Encourage robust products** with fewer weaknesses and vulnerabilities
- **Quality of Service**: Require vendors to guarantee uptime safeguards in the context of denial of service and ransom ware attacks.
  - Ask vendors to include language on minimal uptime in response to a denial of service attack and ransom ware

- **Manage access to sensitive information**: Require vendors to encrypt and authenticate any 3rd party remote access to any critical cyber systems. Require vendors to remain compliant with current version of NIST 800-53 requirements for access controls and remote access.
- **Ensure the product is implemented as specified:** Require vendor to follow secure configuration and integration and provisioning best practices
- **Secure development practices**, including:
  - Quality assurance, quality control, testing, code reviews, timely communication
  - Specifying country of origin: Are there any connections to servers or personnel abroad? If so, where? Are these countries home to advanced persistent threats that frequently target U.S. critical infrastructure?

2.3 General Cybersecurity Procurement Considerations

Regardless of product, general cybersecurity considerations around the below elements should be considered in the procurement process and be tailored and integrated for the environment in which it will be applied:

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

3.0 Elements of a Cybersecurity Procurement Plan

When federal staff are working with suppliers, they should develop a plan that covers procurement, implementation, and integration. For an implementation plan to be considered acceptable, it must address the following:

> *At a minimum, the cybersecurity implementation plan must describe how cybersecurity is established between networks, systems, devices, application or components within the proposed solution, and at the necessary external interfaces at the solution boundaries.*

Additionally, the procurement, implementation, and integration plan should cover the following elements:

- A summary of the cyber security risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact).
- A summary of the cyber security criteria utilized for vendor and device selection.
- A summary of the relevant cyber security standards and/or best practices that will be followed.
- A summary of how the project will support emerging smart grid cyber security standards.
- Plans should also address the adequacy of their approach for addressing
  - Ensuring confidentiality, integrity, availability
  - Secure logging, monitoring, alarming, and notification

3.1 Cybersecurity Assessment Process Considerations

The following list of elements for a Cybersecurity Plan provides suggestions regarding the cybersecurity assessment process and the structure of the plan:

- **Assessment of Scope**: A discussion of the scope of the solution should be made, as well as the anticipated challenges (such as confidentiality, integrity or availability is high, but systems or component resources are low). Implementers should document all the interfaces (where information is exchanged between networks, systems, devices, applications or components) in their proposed solution as a method for assessing the full scope of the plan. It should be noted that an assessment of all interfaces is also required for an Interoperability Plan, and both plans can utilize the same assessment.
- **Content and Format:** A statement of plan for designing in cybersecurity, including a defense in depth approach, and plans for sustaining cybersecurity for the life of the solution. Where existing practice or standards seem inadequate, implementers should propose remedies through open public mechanisms to alleviate them over time. Existing, accepted community standards should be used where possible. Where community standards are missing or inadequate, the plan could propose alternate strategies, and should advise the sponsoring program.

4.0 References

E.O. 13800, 82 FR 22391 (2017). “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”. Accessed February 20, 2019: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

Energy Sector Control Systems Working Group (ESCSWG) (April 2014). “Cybersecurity Procurement Language for Energy Delivery Systems.” Accessed February 20, 2019: https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

U.S. Department of Homeland Security (2009). “Cyber Security Procurement Language for Control Systems.” Accessed February 20, 2019: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf

PNNL- 28661

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov