AGA Cybersecurity Procurement Language Tool: Usage Examples

A Publication for AGA Members

Prepared by the AGA Cybersecurity Strategy Task Force

AGA
American Gas Association

Notice:

In issuing and making this publication available, AGA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is AGA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. The statements in this publication are for general information and represent an unaudited compilation of statistical information that could contain coding or processing errors. AGA makes no warranties, express or implied, nor representations about the accuracy of the information in the publication or its appropriateness for any given purpose or situation.

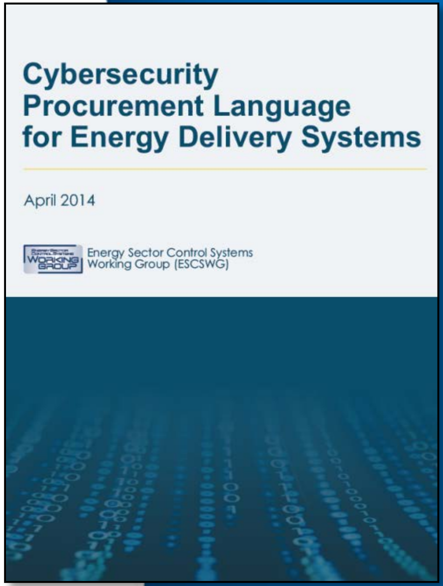
This publication shall not be construed as including, advice, guidance, or recommendations to take, or not to take, any actions or decisions in relation to any matter. Should you take any such action or decision; you do so at your own risk. Information on the topics covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

About This Tool

- The AGA Cybersecurity Strategy Task Force has prepared this tool to assist AGA members with identifying appropriate cybersecurity language to include in procurement contracts
- The specific language provided in this tool is based on the *Cybersecurity Procurement Language for Energy Delivery Systems*, published in April, 2014 jointly by the Energy Sector Control Systems Working Group, the Pacific Northwest National Laboratory, and Energetics Incorporated, with funding from the U.S. Department of Energy
- The accompanying spreadsheet tools helps users identify recommended contract language based on risk tolerance and the type of purchase (e.g., hardware, software, and/or services)

Procurement Language Contents

- The language in this tool is based on the Energy Sector Control Systems Working Group (ESCSWG) *Cybersecurity Procurement Language for Energy Delivery Systems*, which is geared specifically toward technical requirements and includes the following:
    - Section 1: How to use document
    - **Section 2: General cybersecurity language**
    - Section 3: Supplier's cybersecurity life cycle
    - Section 4: Intrusion detection
    - Section 5: Physical security
    - Section 6: Wireless security
    - Section 7: Encryption
- The language in this tool is only based on Section 2



Cybersecurity Procurement Language for Energy Delivery Systems

April 2014

Energy Sector Control Systems Working Group (ESCSWG)

Implementation Process

Type of Contract

Risk Tolerance

	Hardware	Software	Service
High			
Medium			
Low			

Cybersecurity Procurement Language Cautions

- Risk Matrix Mapping was done by Various Team Members – You Control the Risk Matrix mapping for your Risk Appetite – Make it Yours!

- Not all Procurement Language Statements are Meant to be used Verbatim – e.g., Sections Stating “as defined or specified by the Acquirer” – 2.5.5, 2.6.4, and 2.10.3 (or date oriented).

- There are Other Components to the ESCSWG (see slide 4), this Tool is to be used to Simplify Choosing Relevant Procurement Language for Your Particular Purchase Decision

Example 1 - Purchase of a Test/Dev Server for General IT Use

- Server Hardware and Operating System Purchase (2.1 and 2.10)
- On-Site Maintenance Service Included with Purchase **(5.1)**
- Remote Access for Maintenance Vendor is Two Factor On Demand (2.5.5)
- Physical Server Installation, OS Installation, on-going Patching, and Provisioning the Responsibility of the Acquirer. (2.2-2.9)
- Server to be used for General Test/Dev Activities for various Application Development Projects.
- Purchase Considered to be “Low Risk” Based on Role of Device, Totality of Purchase, and Security Implications

Sample Language: Section 2.1

Software and Services Procurement Language Inclusions

2.1.2 “The Supplier shall provide documentation of the 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.”

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

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

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

ESCSWG Procurement Language

Section 2.1: Software Services Language Required

	Hardware	Software	Service
High	2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6	2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6	2.1.2 2.1.3 2.1.4 2.1.5 2.1.6
Medium	2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6	2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6	2.1.2 2.1.3 2.1.4 2.1.5 2.1.6
Low	2.1.2 2.1.4 2.1.5 2.1.6	**2.1.2** **2.1.4** **2.1.5** **2.1.6**	2.1.2 2.1.4 2.1.5 2.1.6

Sample Procurement Language Example 1: Section 2.2–2.9

Since all the baseline Procurement Language in Sections 2.2 to 2.9 refers to implementation activities performed by the internal IT team, then these security elements can be omitted from any procurement contract and (if you want) referred to as an Internal Technical Standard for IT to follow.

Any of the participants in the procurement process can take on multiple roles – in this case the Acquirer takes on the Integrator Role.

Sample Procurement Language Example 1: Section 2.10 Reliability and Adherence to Standards

2.10.1 “The Supplier shall protect the confidentiality and integrity of the Acquirer’s sensitive information.”

From Slide #6 – since the [Purchase Considered to be “Low Risk” Based on Role of Device, Totality of Purchase, and Security Implications], only Procurement Language 2.10.1 applies per the matrix.

ESCSWG Procurement Language

Section 2.10: Reliability and Adherence to Standards

	Hardware	Software	Service
High	2.10.1 2.10.2 2.10.3 2.10.4	2.10.1 2.10.2 2.10.3 2.10.4	2.10.1 2.10.2 2.10.3 2.10.4
Medium	2.10.1 2.10.2 2.10.3 2.10.4	2.10.1 2.10.2 2.10.3 2.10.4	2.10.1 2.10.2 2.10.3 2.10.4
Low	**2.10.1**	2.10.1	2.10.1

Example 2 - Purchase of a Medium Sized SCADA Application Upgrade Including Networking Hardware but not PLC’s or RTU’s.

- Server, Workstation, and Networking Hardware Purchase (2.1 – 2.10)
- OS and SCADA Application Upgrade Purchase (2.1 – 2.10)
- On-Site Maintenance Service Included with Purchase **(5.1)**
- Remote Access for Maintenance Vendor is Two Factor On Demand (2.5.5)
- Physical Server Installation, OS Installation, on-going Patching, and Provisioning the Responsibility of the Integrator. Not an SSO solution (Leaves out 2.5.6 – 2.5.9).
- SCADA Upgrade Project to Replace Existing SCADA Environment after Parallel Implementation Period
- Purchase Considered to be “High Risk Risk” Based on Role of Devices, Totality of Purchase, and Security Implications

ESCSWG Procurement Language

Section 2.1: Software Services

Example 2 SCADA System

	Hardware	Software	Service
High	**2.1.1** **2.1.2** **2.1.3** **2.1.4** **2.1.5** **2.1.6**	**2.1.1** **2.1.2** **2.1.3** **2.1.4** **2.1.5** **2.1.6**	**2.1.2** **2.1.3** **2.1.4** **2.1.5** **2.1.6**
Medium	2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6	2.1.1 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6	2.1.2 2.1.3 2.1.4 2.1.5 2.1.6
Low	2.1.2 2.1.4 2.1.5 2.1.6	2.1.2 2.1.4 2.1.5 2.1.6	2.1.2 2.1.4 2.1.5 2.1.6

Example 2 - Purchase of a Medium Sized SCADA Application Upgrade Including Networking Hardware but not PLC's or RTU's.

- Note that you can include the Recommended Procurement Language where it makes the most sense:

1. Master Services Agreement
2. Statement of Work
3. Purchase Order
4. Internal or Multivendor Project Plan (Requirements Document)
5. Internal Technical Security Standards or Policy

ESCSWG Procurement Language

Section 2.2: Access Control – Example 2 SCADA System

	Hardware	Software	Service
High	**2.2.1** **2.2.2** **2.2.3** **2.2.4** **2.2.5**	**2.2.6** **2.2.7** **2.2.8** **2.2.9**	**2.2.1** **2.2.2** **2.2.3** **2.2.4** **2.2.5**
Medium	2.2.1 2.2.2 2.2.3 2.2.4 2.2.5	2.2.6 2.2.7 2.2.8 2.2.9	2.2.1 2.2.2 2.2.3 2.2.4 2.2.5
Low	2.2.1 2.2.2 2.2.3 2.2.4 2.2.5	2.2.6 2.2.8	2.2.1 2.2.2 2.2.3 2.2.4 2.2.5

ESCSWG Procurement Language

Section 2.3: Account Management

Example 2 SCADA System

	Hardware	Software	Service
High	**2.3.1 2.3.2 2.3.3 2.3.4**	**2.3.1 2.3.2 2.3.3 2.3.4**	**2.3.1 2.3.2 2.3.3 2.3.4**
Medium	2.3.1 2.3.2 2.3.3 2.3.4	2.3.1 2.3.2 2.3.3 2.3.4	2.3.1 2.3.2 2.3.3 2.3.4
Low	2.3.1 2.3.2 2.3.3	2.3.1 2.3.2 2.3.3	2.3.1 2.3.2 2.3.3

ESCSWG Procurement Language

Section 2.4: Session Management

Example 2 SCADA System

	Hardware	Software	Service
High	**2.4.1** **2.4.2** **2.4.3** **2.4.4**	**2.4.1** **2.4.2** **2.4.3** **2.4.4**	**2.4.1** **2.4.2** **2.4.3** **2.4.4**
Medium	2.4.1 2.4.2 2.4.3	2.4.1 2.4.2 2.4.3	2.4.1 2.4.2 2.4.3
Low	2.4.1	2.4.1	2.4.1

ESCSWG Procurement Language

Section 2.5: Authentication/Password Policy Management

Example 2 – SCADA System

	Hardware	Software	Service
High	**2.5.1** **2.5.2** **2.5.3** **2.5.4** **2.5.5**	**2.5.1** **2.5.2** **2.5.3** **2.5.4** **2.5.5**	**2.5.1** **2.5.2** **2.5.3** **2.5.4** **2.5.5**
Medium	2.5.1 2.5.2 2.5.3	2.5.1 2.5.2 2.5.3	2.5.1 2.5.2 2.5.3 2.5.4 2.5.5
Low	2.5.1 2.5.3	2.5.1 2.5.3	2.5.1 2.5.3

ESCSWG Procurement Language

Section 2.5: Single Sign-on Policy Management

Example 2 – SCADA System

	Hardware	Software	Service
High	2.5.6 2.5.7 2.5.8 2.5.9	2.5.6 2.5.7 2.5.8 2.5.9	2.5.6 2.5.7 2.5.8 2.5.9
Medium	2.5.6 2.5.8 2.5.9	2.5.6 2.5.8 2.5.9	2.5.6 2.5.7 2.5.8 2.5.9
Low	2.5.6 2.5.8 2.5.9	2.5.6 2.5.8 2.5.9	2.5.6 2.5.7 2.5.8 2.5.9

ESCSWG Procurement Language

Section 2.6: Account Auditing and Logging

Example 2 – SCADA System

	Hardware	Software	Service
High	**2.6.1** **2.6.2** **2.6.3** **2.6.4** **2.6.5** **2.6.6**	**2.6.1** **2.6.2** **2.6.3** **2.6.4** **2.6.5** **2.6.6**	**2.6.1** **2.6.2** **2.6.3** **2.6.4** **2.6.5** **2.6.6**
Medium	2.6.1 2.6.2 2.6.3 2.6.4 2.6.5 2.6.6	2.6.1 2.6.2 2.6.3 2.6.4 2.6.5 2.6.6	2.6.1 2.6.2 2.6.3 2.6.4 2.6.5 2.6.6
Low	2.6.1 2.6.2 2.6.3 2.6.4 2.6.5 2.6.6	2.6.1 2.6.2 2.6.3 2.6.4 2.6.5 2.6.6	2.6.1 2.6.2 2.6.3 2.6.4 2.6.5 2.6.6

ESCSWG Procurement Language

Section 2.7: Communications Restrictions

Example 2 – SCADA System

	Hardware	Software	Service
High	**2.7.1 to 2.7.10** **2.7.13** **2.7.14** **2.7.15**	**2.7.1 to 2.7.5** **2.7.13** **2.7.14** **2.7.15**	**2.7.1 to 2.7.6** **2.7.10** **2.7.13** **2.7.14** **2.7.15**
Medium	2.7.1 to 2.7.10 2.7.13 2.7.14 2.7.15	2.7.1 to 2.7.5 2.7.13 2.7.14 2.7.15	2.7.1 to 2.7.6 2.7.10 2.7.13 2.7.14 2.7.15
Low	2.7.1 to 2.7.10 2.7.13 2.7.14 2.7.15	2.7.1 to 2.7.5 2.7.13 2.7.14 2.7.15	2.7.1 to 2.7.6 2.7.10 2.7.13 2.7.14 2.7.15

ESCSWG Procurement Language

Section 2.8: Malware Detection and Protection

Example 2 – SCADA System

	Hardware	Software	Service
High	**2.8.1** **2.8.2** **2.8.3**	**2.8.2** **2.8.3**	**2.8.2** **2.8.3**
Medium	2.8.1 2.8.2 2.8.3	2.8.2 2.8.3	2.8.2 2.8.3
Low	2.8.1		

ESCSWG Procurement Language

Section 2.9: Heartbeat Signals

Example 2 – SCADA System

	Hardware	Software	Service
High	**2.9.1** **2.9.2**		
Medium	2.9.1 2.9.2		
Low	2.9.1 2.9.2		

ESCSWG Procurement Language

Section 2.10: Reliability and Adherence to Standards

Example 2 – SCADA System

	Hardware	Software	Service
High	**2.10.1** **2.10.2** **2.10.3** **2.10.4**	**2.10.1** **2.10.2** **2.10.3** **2.10.4**	**2.10.1** **2.10.2** **2.10.3** **2.10.4**
Medium	2.10.1 2.10.2 2.10.3 2.10.4	2.10.1 2.10.2 2.10.3 2.10.4	2.10.1 2.10.2 2.10.3 2.10.4
Low	2.10.1	2.10.1	2.10.1