Release of the Draft Cybersecurity Procurement Language for Energy Delivery Systems

Energy Sector Control Systems Working Group
Supporting the Electricity Sector Coordinating Council, Oil & Natural Gas Sector Coordinating Council, and Government Coordinating Council for Energy

October 28, 2013
Agenda

• Rationale
• Document overview
• Alignment with the energy sector roadmap
• Core team members
• Approach and differences
• Instructions for commenting
• Role for stakeholders
• Next steps
Why Procurement Language for the Energy Sector?

→ The energy sector continues to evolve as it faces:
  – New cybersecurity threats
  – Changes in security practices and requirements
  – Advancing technologies

→ Asset owners and operators are experiencing increased pressure for meeting stringent regulatory requirements
  – Acquirers, integrators, and suppliers need to communicate expectations and requirements in a clear and repeatable manner

→ A number of procurement language guidance documents exist, but understanding how to effectively use them can be confusing
What is the Cybersecurity Procurement Language for Energy Delivery Systems?

This document seeks to promote cybersecurity by design through procurement language tailored to the specific needs of the energy sector.

Highlights:

• Provides baseline cybersecurity requirements that can be used in the procurement of energy delivery systems and components.

• Intended to:
  — Address current technological advancements and challenges of the energy sector.
  — Help energy sector stakeholders more clearly communicate expectations and requirements.

• Not intended to be inserted verbatim into procurement contracts.
Meeting the Vision of the Roadmap to Achieve Energy Delivery Systems Cybersecurity

Roadmap Vision

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

- Developed by the Energy Sector Control Systems Working Group (ESCSWG) for asset owners, operators, government, regulators, standards bodies, researchers, academia, vendors and other solution providers
- Synthesis of energy delivery systems security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in energy delivery systems security

For more information visit: www.controlsystemsroadmap.net
### Alignment with Roadmap Strategies

<table>
<thead>
<tr>
<th>Near-term (0-3 yrs)</th>
<th>Mid-term (4-7 years)</th>
<th>Long-term (8-10 years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Executive engagement and support of cyber resilience efforts</td>
<td>1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available</td>
<td>1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry</td>
</tr>
<tr>
<td>1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched</td>
<td>1.4 Field-proven best practices for energy delivery systems security widely employed</td>
<td>2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available</td>
</tr>
<tr>
<td>2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings</td>
<td>2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics</td>
<td>3.4 Self-configuring energy delivery system network architectures widely available</td>
</tr>
<tr>
<td>3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available</td>
<td>3.2 Scalable access control for all energy delivery system devices available</td>
<td>3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions</td>
</tr>
<tr>
<td>4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available</td>
<td>4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available</td>
<td>4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector</td>
</tr>
<tr>
<td>4.3 Incident reporting guidelines accepted and implemented by each energy subsector</td>
<td>5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders</td>
<td>5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems</td>
</tr>
<tr>
<td>5.2 Federal and state incentives available to accelerate investment in resilient energy delivery systems</td>
<td>4.4 Real-time forensics capabilities commercially available</td>
<td>5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector</td>
</tr>
<tr>
<td>5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners</td>
<td>4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available</td>
<td><strong>Alignment with Roadmap Strategies</strong></td>
</tr>
<tr>
<td>5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining</td>
<td><strong>Alignment with Roadmap Strategies</strong></td>
<td><strong>Alignment with Roadmap Strategies</strong></td>
</tr>
</tbody>
</table>
## Building a Culture of Security

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Near-term (0–3 yrs)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 Executive engagement and support of cyber resilience efforts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mid-term (4–7 yrs)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4 Field-proven best practices for energy delivery systems security widely employed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 Compelling business case developed for investment in energy delivery systems security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Long-term (8–10 yrs)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Risk** measures subsector security settings
- **Assess and Monitor Risk** includes state assessment tools across all energy delivery systems
- **Develop and Implement New Protective Measures** includes scalable access control for all energy delivery system devices
- **Manage Incidents** includes incident reporting guidelines
- **Sustain Security Improvements** focuses on developing cybersecurity solutions for energy delivery systems

### Improvements
- **1.1** Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available
- **3.1** Scalable access control for all energy delivery system devices
- **3.2** Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented
- **4.1** Tools to identify cyber events across all levels of energy delivery system networks commercially available
- **4.2** Tools to support and implement cyber attack response decision making for the human operator commercially available
- **5.1** Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders
- **5.2** Federal and state incentives available to accelerate investment in resilient energy delivery systems
- **5.3** Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners
- **5.4** Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining
- **5.5** Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems
- **5.6** Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector
Behind the Scenes

- **ESCSWG**: Leading this effort, spearheaded by Ed Goff (Duke Energy)
- **Pacific Northwest National Laboratory (PNNL)**: Assisted with the facilitation and writing
- **U.S. Department of Energy**: Provided leadership, guidance, funding, and support to facilitate the development of this document
- **Energetics Incorporated**: Assisted with facilitation, coordination, and public outreach
- **Core Team of Technical Advisors**: Volunteered significant time and expertise in advising the drafting of this first draft. Core team includes representatives from:
Development Approach

- Providing for open, transparent, and formal public review cycles
- Engaging energy sector stakeholders from acquirer, integrator, and supplier communities
- Built on the *Department of Homeland Security Cyber Security Procurement Language for Control Systems* (DHS, 2009) to tailor guidance to the specific needs of the energy sector
  - Addressed baseline cybersecurity requirements (not all-inclusive)
  - Updated language to address technological advancements
  - Laser focused on procurement language
  - Focused on “what to do”, not “how to do it”
  - Minimized redundancies
- Reviewed other existing documents and approaches to understand how they complement each other as well as identify gaps or opportunities to address unique energy sector challenges
What Is Different?

• The new draft document is 20% the size of the original DHS (2009) document
• Redundancy is minimized
  – Near identical requirements that were presented in multiple sections are reduced
• Technical approaches are modernized
• Explanations of specific technologies have been removed
• Accounts for the differences in acquiring components and energy delivery systems
Differences (cont)

• Focuses on energy sector needs
• Removed detailed Factory and Site Acceptance Testing and Maintenance Guidance
• Similar concepts are grouped together in only a few sections

**DHS (2009)**
- System Hardening (with 6 sections)
- Perimeter Protection (3 sections)
- Account Management (7 sections)
- Coding Practices (1 section)
- Flaw Remediation (2 sections)
- Malware Detection and Protection (1 section)
- Host Name Resolution (1 section)
- End Devices (4 sections)
- Remote Access (6 sections)
- Physical Security (4 sections)
- Network Partitioning (2 sections)
- Wireless Technologies (11 sections)

**Draft EDS PL**
- General Procurement Language (12 sections)
- Supplier’s Lifecycle Security Program (6 sections)
- Intrusion Detection (2 sections)
- Physical Security (3 sections)
- Wireless Security (2 sections)
Sample Update

**Wireless Technologies**

- DHS (2009) has 27 pages devoted to this topic and 105 procurement language items
- EDS PL has 2 pages and only 12 procurement language items

---

**DHS (2009) WIRELESS TECHNOLOGIES**

1. Bluetooth
2. Wireless Closed Circuit TV
3. Radio Frequency Identification
4. 802.11
5. ZigBee
6. WirelessHART
7. Mobile Radios
8. Wireless Mesh Networks
9. Cellular
10. WiMAX
11. Microwave
12. Satellite

---

**Draft EDS PL WIRELESS TECHNOLOGIES**

1. General Wireless
2. Specialized Wireless
## Project Timeline

### 2013-2014

<table>
<thead>
<tr>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gap Analysis</td>
<td></td>
<td></td>
<td></td>
<td>Data Collection &amp; Synthesis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Draft PL Document &amp; Internal Review</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Collect and Review Stakeholder Comments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Stakeholder Comment Period Nov. 6 – Dec. 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Prepare Final PL Doc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Stakeholder Outreach**
Instructions for Commenting

1. Draft will be posted on **November 6**. Visit: [www.controlsystemsroadmap.net](http://www.controlsystemsroadmap.net) and see “News”

2. Download *Draft Cybersecurity Procurement Language for Energy Delivery Systems* document and supporting comment matrix

3. Submit comments by **December 6** to es-pl@energetics.com

<table>
<thead>
<tr>
<th>Line(s)</th>
<th>Comment</th>
<th>Recommended Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We Need Your Feedback

• We can’t do this without your feedback!
  – Electric/ONG: Acquirers, suppliers, integrators

• Need to know how this document would be helpful with your procurements and what might be missing

• Please share with friends and colleagues

• Comments due December 6
Next Steps

• Planning communication and rollout
  – Context based – supplier, acquirer, & integrator
  – Point of contact for questions
  – Long-term maintenance plan

• Future Phase:
  – Expand on implementation guidance
  – Coordinate with stakeholder groups to align to other existing methodologies, standards, and practices
Questions?

For more information visit: https://www.controlsystemsroadmap.net/efforts/Pages/Cybersecurity-Procurement-Language-for-Energy-Delivery-Systems.aspx