Electricity Subsector
Cybersecurity Capability Maturity Model (ES-C2M2)

Patricia Hoffman
Assistant Secretary
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy
www.OE.energy.gov
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

- ES-C2M2 enables consistent evaluation of the maturity of an organization’s cybersecurity capabilities; allowing the entity to prioritize its cybersecurity investments.


- ES-C2M2 program information can be obtained by emailing ES-C2M2@HQ.DOE.GOV
ES-C2M2 Program Metrics

• 2012
  – JAN: Program kickoff
  – APR: 17 Pilot Facilitations
  – MAY: Functional Model Developed
  – MAY – DEC: 7 DOE Facilitated Self-Evaluations

• 2013
  – JAN – FEB: 1 DOE Facilitated Self-Evaluation

• ES-C2M2 toolkit requests
  – 199 requests since June 2012
  – 103 utilities, 17 international, 79 non-utilities
Cyber Security Framework

Comprised of Capability and Risk Management

- Risk Management (analyze risk)
- Asset Configuration Management (inventory, architecture, software upgrades)
- Identity and Access Management (role base access for application and physical access)
- Threat and Vulnerability Management (new IT, OT technologies)
- Situational Awareness (Monitoring tools, intrusion detection tools)
- Information Sharing and Communications
- Event and Incident Response (Detect and Respond)
- Supply Chain and External Dependencies Management
- Workforce Management
• Situational awareness activities may include:
  – Performance of logging
  – Monitoring logs
  – Aggregating monitoring information
  – Developing a “Common Operating Picture”

• Example MIL Progression for “Monitor the Function”
  – MIL1 – Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)
  – MIL2 – Alarms and alerts are configured to aid the identification of cybersecurity events
  – MIL3 – Continuous monitoring is performed across the operational environment to identify anomalous activity
Incident response activities may include:

- Analyzing incidents to identify patterns and trends
- Logging, tracking and reporting incidents
- Performing root-cause and lessons-learned analysis

Example MIL Progression for “Plan for Continuity”

- MIL1 – The sequence of activities necessary to return the function to normal operation is identified
- MIL2 – Recovery time objectives for the function are incorporated into continuity plans
- MIL3 – Recovery time objectives are aligned with the function’s risk criteria
**Example: Shodan**

*Description: Readily available search engine that identifies configuration of industrial control systems connected to the internet*

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Accessible assets</td>
<td>A network (IT and/or OT) architecture is used to support risk analysis</td>
</tr>
<tr>
<td>Remote Access</td>
<td>Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring</td>
</tr>
<tr>
<td>Brute Force Attack</td>
<td>Anomalous access attempts are monitored as indicators of cybersecurity events</td>
</tr>
<tr>
<td>Known Vulnerability Exploits</td>
<td>Cybersecurity vulnerability information is gathered and interpreted for the function</td>
</tr>
</tbody>
</table>
### Example: Night Dragon

**Description:** Coordinated attack by Advanced Persistent Threat using multiple attack vectors with the goal of data theft

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Engineering</td>
<td>Cybersecurity awareness content is based on the organization’s threat profile, users are educated</td>
</tr>
<tr>
<td>Default Hardware</td>
<td>The design of configuration baselines includes cybersecurity objectives</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Known Vulnerability</td>
<td>Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function, at an organization-defined frequency</td>
</tr>
<tr>
<td>Exploits</td>
<td></td>
</tr>
<tr>
<td>Lack of awareness</td>
<td>Information sources to support threat management activities are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings)</td>
</tr>
</tbody>
</table>

R&D Success Story: Lemnos Interoperable Configuration Profiles

Today, at least ten vendors of power grid devices have implemented the Lemnos solution for interoperable cybersecurity of energy sector routable communications

- **Secure channels for routable data communications** through Internet Protocol Security (IPSec) virtual private networks (VPNs)
- **Secure web communications and terminal connection** using the Transport Layer Security (TLS) cryptographic protocol to provide communication security over the Internet and Secure Shell (SSH) for public-key cryptography to authenticate a remote terminal user
- **Centralized Certificate Revocation** using the Online Certificate Status Protocol (OCSP) to obtain the revocation status of a digital certificate
- **Central authentication and authorization** using the Lightweight Directory Access Protocol (LDAP) for accessing and maintaining distributed directory information services over an IP network
- **Central log collection** using Syslog for notification, traceability, and trouble shooting

**Project Team:** EnerNex Corporation, Sandia National Laboratories, Schweitzer Engineering Laboratories, Tennessee Valley Authority

**Project Partners:**
- EnerNex Corporation
- Sandia National Laboratories
- Schweitzer Engineering Laboratories
- Tennessee Valley Authority

**Vendors Using Lemnos:**
- Industrial Defender
- Cisco
- n-dimensional solutions
- Siemens
- Phoenix Contact
- encore-networks™
- RUGGEDCOM
- GarrettCom
R&D Success Story: exe-Guard

Protects substation servers and communication processors against malware and unauthorized changes

- Whitelisting solution for embedded Linux® devices
- Protects against malware at the device level
- Maintains settings and configuration integrity
- Minimizes application of security patches
- Addresses CIP-007-R4, which requires asset owners to employ malicious software prevention tools on assets
- Addresses the CIP-007-R3 requirement for security patch management

Technical Approach

- Develop a software solution for embedded Linux Systems
- Leverage deny by default/whitelist approach
- Implements Autoscopy Jr. developed by the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) for kernel hardening

For more information:
https://www.controlsystemsroadmap.net/Efforts/Pages/exe-Guard.aspx

Project Team: Schweitzer Engineering Laboratory, Dominion Virginia Power, Sandia National Laboratories
Additional Information

NIST Request for Information
• https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity

Cybersecurity Executive Order

• Electricity Subsector Cybersecurity Capability Maturity Model
Backup Slides
Examples of DOE National Laboratory R&D to enhance cybersecurity in energy sector

1. **High-Level (4th Gen) Language Microcontroller Implementation** – Idaho National Laboratory is implementing a high-level fourth generation programming language for use with microcontrollers that limits direct access to device memory and hardens microcontrollers against low-level cyber attacks

   **Partners:** Siemens Corporate Research

2. **Control Systems Situational Awareness Technology Interoperable Tool Suite** – Idaho National Laboratory is developing a situational awareness tool suite for control systems

   **Partners:** Idaho Falls Power, Austin Energy, Argonne National Laboratory, University of Illinois, Oak Ridge National Laboratory, University of Idaho

3. **Automated Vulnerability Detection for Compiled Smart Grid Software** – Oak Ridge National Laboratory is developing a system for conducting cybersecurity vulnerability detection of smart grid components and systems by performing static analysis of compiled software and device firmware

   **Partners:** Software Engineering Institute, University of Southern Florida, EnerNex Corporation

4. **Next Generation Secure, Scalable Communication Network for the Smart Grid** – Oak Ridge National Laboratory is developing a wireless technology that is robust, secure, scalable for smart grid applications using an adaptive hybrid spread-spectrum modulation format to provide superior resistance to multipath, noise, interference, and jamming

   **Partners:** Pacific Northwest National Laboratory, Virginia Tech, OPUS Consulting, Kenexis Consulting.

5. **Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector** – Pacific Northwest National Laboratory is demonstrating that a bio-inspired solution using lightweight, mobile agents (Digital Ants) can be deployed across multiple organizational boundaries found in smart grid architectures to correlate activities, produce emergent behavior, and draw attention to anomalous condition

   **Partners:** Wake Forest University, University of California-Davis, Argonne National Laboratory, SRI International.
Examples of Applied R&D to Enhance Energy Sector Cybersecurity

1. **Watchdog** – Schweitzer Engineering Laboratories is developing a Managed Switch for the control system local area network (LAN) that performs deep packet inspection using a white list configuration approach to establish a set of known, allowed communications

   **Partners:** CenterPoint Energy Houston Electric, Pacific Northwest National Laboratory

2. **Padlock** - Schweitzer Engineering Laboratories is developing a security gateway to help protect field device communications and sense physical tampering to enhance cyber and physical security at the distribution network level. The low-power, low-cost Padlock Gateway will establish encrypted communication between central stations and filed devices while enabling strong access controls, logging, and secure communications with transparent access to the serial port of the existing energy system protection device

   **Partners:** Tennessee Valley Authority, Sandia National Laboratories

3. **Role Based Access Control -Driven (RBAC) Least Privilege Architecture for Control Systems** – Honeywell International is developing a role based access control driven least privilege architecture for energy delivery systems

   **Partners:** University of Illinois, Idaho National Laboratory

4. **SIEGate** – Grid Protection Alliance is developing a Secure Information Exchange Gateway (SIEGate) that provides secure communication of data between control centers

   **Partners:** University of Illinois, Pacific Northwest National Laboratory, PJM, AREVA T&D.

5. **Smart Grid Cryptographic Key Management** – Sypris Electronics is developing a cryptographic key management system scaled to secure communications for the millions of smart meters within the smart grid advanced metering infrastructure

   **Partners:** Purdue University Center for Education and Research in Information Assurance and Security, Oak Ridge National Laboratory, Electric Power Research Institute
ES-C2M2 Model Structure

- **Risk Management**
- **Asset, Change, and Configuration Management**
- **Identity and Access Management**
- **Threat and Vulnerability Management**
- **Situational Awareness**
- **Information Sharing and Communications**
- **Event and Incident Response, Continuity of Operations**
- **Supply Chain and External Dependencies Management**
- **Workforce Management**
- **Cybersecurity Program Management**

- Domains are logical groupings of Cybersecurity practices
- Each domain has a short name for easy reference