Participating Organizations:

- Edison Electric Institute
- American Public Power Association
- Pacific Northwest Laboratory
- Idaho National Laboratory

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Program

Program Overview

ES-C2M2 Background & Overview

• **Challenge**: Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid

**ES-C2M2 Objectives**

• Strengthen cybersecurity capabilities
• Enable consistent evaluation and benchmarking of cybersecurity capabilities
• Share knowledge and best practices
• Enable prioritized actions and cybersecurity investments
ES-C2M2 Domains

- **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**

ES-C2M2 Capability Development Illustration

**Access, Change and Configuration Management Example**

- Access control activities may include:
  - Unique accounts vs. shared accounts
  - Access limited to specific assets, during a specified maintenance interval
  - Use single or multifactor authentication

- Example MIL Progression for “Control Access”
  - MIL1 – Access requirements, including those for remote access, are determined (which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)
  - MIL2 – Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring
  - MIL3 – Anomalous access attempts are monitored as indicators of cybersecurity events
ES-C2M2 Capability Development Illustration

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>ES-C2M2 Practice</th>
<th>ES-C2M2 Domain</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>
<td>RISK</td>
</tr>
<tr>
<td>Remote Access</td>
<td>Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring</td>
<td>ACCESS</td>
</tr>
<tr>
<td>Brute Force Attack</td>
<td>Anomalous access attempts are monitored as indicators of cybersecurity events</td>
<td>ACCESS</td>
</tr>
<tr>
<td>Known Vulnerability Exploits</td>
<td>Cybersecurity vulnerability information is gathered and interpreted for the function</td>
<td>THREAT</td>
</tr>
</tbody>
</table>


Sample Report Results

2 Control Access

MIL1
a. Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)
b. Access is granted to identities based on requirements
c. Access is revoked when no longer required

MIL2
d. Access requirements incorporate least privilege and separation of duties principles
e. Access requests are reviewed and approved by the asset owner
f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring

MIL3
g. Access privileges are reviewed and updated to ensure validity, at an organizationally-defined interval
h. Access to assets is granted by the asset owner based on risk to the function
i. Anomalous access attempts are monitored as indicators of cybersecurity events
Notional Sample Report
Actual vs. Desired Score

Industry Scores vs. Organization
ES-C2M2: Industry Use and Adoption

- Over 120 requests
  - 70+ utilities, 8 international, 40+ non-utilities
- Utilities have begun self assessments
  - Identification of desired baselines
  - Prioritization of investment based on comparison of results to desired baseline
  - Use of 3rd Parties for implementation and “Deep Dives” into specific domains

ES-C2M2: Approaches for Use

- DOE Facilitation
  - Model designers on site to facilitate discussion
- Leveraging 3rd Parties
  - Avoid mapping of ES-C2M2 practices overttop of current methodology
    - Potential misinterpretation of model concepts
ES-C2M2: Future Potential

- Share Best Practices within the sector
- Identify approaches for Capability Development
- Discussion Opportunities created
- Develop anonymous aggregated Benchmarking Data
- R&D Investment needs identified by result data
- Access to Online Training Tools

Links

ES-C2M2 Model

ES-C2M2 Self-Evaluation Tool Requests, Questions, or Requests for Facilitation
ES-C2M2@doe.gov
Background Slides

ES-C2M2 Capability Development Illustration

Threat and Vulnerability Management Example

- Threat and vulnerability management activities may include:
  - Gathering information on related threats and vulnerabilities from sources such as trusted partners, ES-ISAC or ICS-CERT
  - Performing network scans and technical security assessments
  - Monitoring for identified threats
  - Participating in cybersecurity exercises, and independent assessments

- Example Progression for “Reduce Cybersecurity Vulnerabilities”
  - MIL1 – Information sources to support cybersecurity vulnerability discovery are identified
  - MIL2 – Cybersecurity vulnerability assessments are performed
  - MIL3 - Cybersecurity vulnerability assessments are tailored based on risk criteria such as impact threshold, recent threat information, or specific vulnerability discoveries
**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>ES-C2M2 Practice</th>
<th>ES-C2M2 Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Engineering</td>
<td>Cybersecurity awareness content is based on the organization’s threat profile</td>
<td>WORKFORCE</td>
</tr>
<tr>
<td>Default Hardware</td>
<td>The design of configuration baselines includes cybersecurity objectives</td>
<td>ASSET</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Known Vulnerability</td>
<td>Cybersecurity vulnerability assessments are performed for all assets important to</td>
<td>THREAT</td>
</tr>
<tr>
<td>Exploits</td>
<td>the delivery of the function, at an organization-defined frequency</td>
<td></td>
</tr>
<tr>
<td>Lack of awareness</td>
<td>Information sources to support threat management activities are identified (e.g.,</td>
<td>THREAT</td>
</tr>
<tr>
<td></td>
<td>ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings)</td>
<td></td>
</tr>
</tbody>
</table>

ES-ISAC Industry Advisory: [http://www.esisac.com/Public%20Library/Alerts/Night%20Dragon.pdf](http://www.esisac.com/Public%20Library/Alerts/Night%20Dragon.pdf)

**Sample Report Results**

1. **Reduce Cybersecurity Vulnerabilities**
   a. Information sources to support cybersecurity vulnerability discovery are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments)
   b. Cybersecurity vulnerability information is gathered and interpreted for the function
   c. Cybersecurity vulnerability information sources that address all assets important to the function are monitored
   d. Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools)
   e. Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function, at an organization-defined frequency
   f. Cybersecurity vulnerability assessments are informed by the function’s (or organization’s) risk criteria (RISK-1c)
### ES-C2M2 Domain Descriptions

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Risk Management (RISK)**                  | Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders. RISK comprises three objectives:  
   1. Establish Cybersecurity Risk Management Strategy  
   2. Manage Cybersecurity Risk  
   3. Manage RISK Activities                                                                                                               |
| **Asset, Change, and Configuration Management (ASSET)** | Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives. ASSET comprises four objectives:  
   1. Manage Asset Inventory  
   2. Manage Asset Configuration  
   3. Manage Changes to Assets  
   4. Manage ASSET Activities                                                                                                               |

### ES-C2M2 Domain Descriptions

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Identity and Access Management (ACCESS)** | Create and manage identities for entities that may be granted logical or physical access to the organization’s assets. Control access to the organization’s assets, commensurate with the risk to critical infrastructure and organizational objectives. ACCESS comprises three objectives:  
   1. Establish and Maintain Identities  
   2. Control Access  
   3. Manage ACCESS Activities                                                                                                               |
| **Threat and Vulnerability Management (THREAT)** | Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization’s infrastructure (e.g., critical, IT, operational) and organizational objectives. THREAT comprises three objectives:  
   1. Identify and Respond to Threats  
   2. Reduce Cybersecurity Vulnerabilities  
   3. Manage THREAT Activities                                                                                                               |
### Domain Description

#### Situational Awareness (SITUATION)

Establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP), commensurate with the risk to critical infrastructure and organizational objectives.

SITUATION comprises four objectives:

1. Perform Logging
2. Monitor the Function
3. Establish and Maintain a Common Operating Picture
4. Manage SITUATION Activities

#### Information Sharing and Communications (SHARING)

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

SHARING comprises two objectives:

1. Share Cybersecurity Information
2. Manage SHARING Activities

#### Event and Incident Response, Continuity of Operations (RESPONSE)

Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

RESPONSE comprises five objectives:

1. Detect Cybersecurity Events
2. Escalate Cybersecurity Events
3. Respond to Escalated Cybersecurity Events
4. Plan for Continuity
5. Manage RESPONSE Activities

#### Supply Chain and External Dependencies Management (DEPENDENCIES)

Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

DEPENDENCIES comprises three objectives:

1. Identify Dependencies
2. Manage Dependency Risk
3. Manage DEPENDENCIES Activities
## ES-C2M2 Domain Descriptions

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Workforce Management (WORKFORCE)** | Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives. WORKFORCE comprises five objectives:  
  1. Assign Cybersecurity Responsibilities  
  2. Control the Workforce Lifecycle  
  3. Develop Cybersecurity Workforce  
  4. Increase Cybersecurity Awareness  
  5. Manage WORKFORCE Activities |
| **Cybersecurity Program Management (CYBER)** | Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure. CYBER comprises five objectives:  
  1. Establish Cybersecurity Program Strategy  
  2. Sponsor Cybersecurity Program  
  3. Establish and Maintain Cybersecurity Architecture  
  4. Perform Secure Software Development  
  5. Manage CYBER Activities |