Evaluating and Improving Cyber Resilience Capabilities of the Electricity and Oil & Natural Gas Critical Infrastructure Components

James Stevens and Dr. Nader Mehravari
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Jason D. Christopher
U.S. Department of Energy
1000 Independence Ave., SW,
Washington, DC, 20585

Abstract – **This paper introduces the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the Oil & Natural Gas Cybersecurity Capability Maturity Model (ONG-C2M2). They are proven tools which allow owners and operators of components of electricity and oil & natural gas critical infrastructure to assess their cybersecurity and resilience capabilities and prioritize their actions and investments to improve cybersecurity and resilience. It combines elements from existing cybersecurity and resilience management efforts into a common tool that can be used consistently across the industry.**

The ES-C2M2 program was established as part of a White House initiative led by the Department of Energy in partnership with the Department of Homeland Security (DHS) and involved close collaboration with representatives from asset owners and operators within the energy sector as well as from industry, private sector, public sector, and other stakeholders.

The goal of this model and associated tools are to support ongoing development and measurement of cybersecurity and resilience capabilities within the energy sector through the following four objectives: (1) Strengthen cybersecurity capabilities in the energy sector, (2) Enable utilities to effectively and consistently evaluate cybersecurity capabilities, (3) Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities, and (4) Enable utilities to prioritize actions and investments to improve cybersecurity.

Keywords *– Operational Resilience, Critical Infrastructure, Resilience Management, Cybersecurity, ES-C2M2, ONG-C2M2*

I. Extended Abstract

The Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2) is designed to help organizations of all types and sizes evaluate and make improvements to their cybersecurity and cyber resilience programs. C2M2 focuses on the implementation and management of cybersecurity and resilience management practices associated with information technology and operations technology assets and the environments in which they operate.

C2M2 is an example of a model derived from the CERT® Resilience Management Model (CERT-RMM) [1], a capability-focused maturity model for improving operational resilience and risk management processes. CERT-RMM served as a foundation for C2M2 because it could be easily customized for the energy sector and because of its systematic approach to managing operational resilience, which is an organization's ability to perform its mission in the presence of operational stress and disruption. The national and economic security of the United States depends on the reliable functioning of the nation's critical infrastructure in the face of increasing cyber threats.

The C2M2 Program [2] was established to address the White House's objective to improve Electricity Subsector (ES) cybersecurity capabilities and to understand the cybersecurity posture of the grid. The first version of the model, ES-C2M2, was released in collaboration with subject matter experts from ES owners and operators, industry groups, and the government [3]. The SEI served as the model architect for ES-C2M2. The overall concept of ES-C2M2 is summarized in Table 1 below.

ES-C2M2 at a Glance	
Sponsor	❖ Department of Energy (DOE)
Target User Organizations	❖ All electric utilities and grid operators, regardless of ownership structure, size, or function
Challenge	❖ Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid
Objectives	❖ Strengthen cybersecurity capabilities ❖ Enable consistent evaluation and benchmarking of cybersecurity capabilities ❖ Share knowledge and best practices ❖ Enable prioritized actions and cybersecurity investments

Table 1 – Overall Concept of ES-C2M2

The DOE, with support from the SEI, also created a version of the model tailored for the Oil and Natural Gas (ONG) Subsector, the ONG-C2M2 [4]. In 2013, the DOE, with support from the SEI, developed a sector-agnostic core model, the C2M2, that can be efficiently tailored for any energy subsector and that can also be used as is by members of other critical infrastructure sectors.

The model is comprised of 10 domains and four maturity indicator levels (MILs). The overall structure of the model and the associated domains are depicted in Figure 2 below.

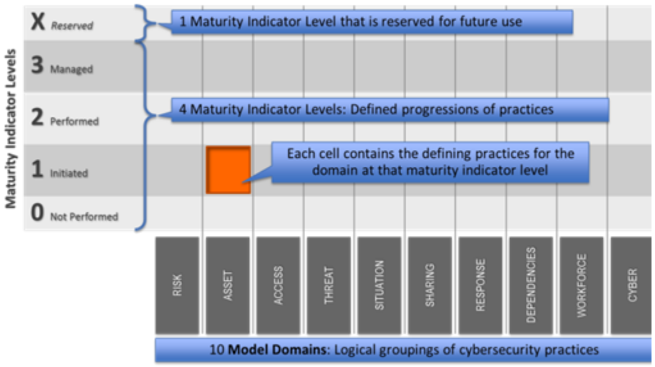
Maturity Indicator Levels
X Reserved
3 Managed
2 Performed
1 Initiated
0 Not Performed
1 Maturity Indicator Level that is reserved for future use
4 Maturity Indicator Levels: Defined progressions of practices
Each cell contains the defining practices for the domain at that maturity indicator level
RISK
ASSET
ACCESS
THREAT
SITUATION
SHARING
RESPONSE
DEPENDENCIES
WORKFORCE
CYBER
10 **Model Domains**: Logical groupings of cybersecurity practices

Figure 2 – Overall Architecture of the C2M2 Model

The description of the 10 domains is as follows:

- **Risk Management:** 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.

- **Asset, Change, and Configuration Management:** Manage the organization's information technology and operations technology assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.

- **Identity and Access Management:** 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.

- **Threat and Vulnerability Management:** Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to critical infrastructure and organizational objectives.

- **Situational Awareness:** Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture.

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

- **Event and Incident Response, Continuity of Operations:** Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cyber event, commensurate with the risk to critical infrastructure and organizational objectives.

- **Supply Chain and External Dependencies Management:** Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the organization's business and security objectives.

- **Workforce Management:** 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.

- **Cybersecurity Program Management:** 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.

C2M2 is a dual progression model there two things are progressing across the maturity indicator levels:

1. **Institutionalization** – the extent to which the practices are ingrained in the organization's operations, and
2. **Approach** – the completeness, thoroughness, or level of development/sophistication of the activity.

One progression describes the completeness, thoroughness, or level of development of the practices in a given domain. The second progression describes the institutionalization of the practices, or how ingrained they are in an organization's operations and way of conducting business. Progression through each domain is measured in four maturity indicator levels, MIL0 through MIL3. Organizations can establish a target MIL for each domain to guide their cybersecurity program improvement.

II. References

[1] CERT-RMM website: http://www.cert.org/resilience/products-services/cert-rmm/cert-rmm-model.cfm

[2] C2M2 Program website: http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program

[3] ES-C2M2 website:
http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2

[4] ONG website: http://energy.gov/oe/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-ong-c2m2