6450-01-P

DEPARTMENT OF ENERGY

Request for Comment on the DOE Cybersecurity Capability Maturity Model Version 2.0

AGENCY: Office of Cybersecurity, Energy Security, and Emergency Response; Department of Energy.

ACTION: Notice of availability; request for comment.

SUMMARY: Through this notice, the Department of Energy (DOE) seeks comments and information from the public on enhancements to the Cybersecurity Capability Maturity Model (C2M2) Version 2.0. C2M2 Version 2.0 incorporates enhancements to align model domains and functional questions with internationally-recognized cyber standards and best practices, including the NIST Cybersecurity Framework Version 1.1 released in April 2018. Since C2M2's last update, new cybersecurity standards have been developed and existing standards have improved. Both technology and threat actors have become more sophisticated, creating new attack vectors and introducing new risks. DOE intends to address these challenges in version 2.0 of C2M2.

DATES: Comments and information are requested by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].**

ADDRESSES: Copies of the draft maturity model are available for public inspection at the U.S. Department of Energy, Forrestal Building, 1000 Independence Avenue, SW., Washington, DC 20585-0121. Public inspection can be conducted between 9:00 a.m. and 4:00 p.m., Monday through Friday, except Federal holidays. These documents can also be accessed online at *http://www.energy.gov/*.

FOR FURTHER INFORMATION CONTACT:

Mr. Timothy Kocher, Special Advisor, U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Forrestal Building, 1000 Independence Avenue, SW., Washington, DC 20585-0121. Tel.: (202) 586-5281. E-mail: *timothy.kocher@hq.doe.gov*.

SUPPLEMENTARY INFORMATION:

C2M2 Version 2.0 leverages and builds upon existing efforts, models, and cybersecurity best practices to advance the model by adjusting to new technologies, practices, and environmental factors. The initiative also accounts for the strategic guidance of EO 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* and EO 13636, *Improving Critical Infrastructure Cybersecurity,* aiming to strengthen and improve the nation's cyber posture and capabilities and to reinforce systematic security and resilience. As industry's use of networked technologies has grown, malicious actors have increasingly targeted the safe and reliable supply of energy. These challenges, along with the evolution of cyber practices, necessitated the C2M2 Version 2.0 update.

A *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. Model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline.

A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. Also, when a model is widely used in a particular industry (and assessment results are shared), organizations can benchmark their performance against other organizations. An industry can determine how well it is performing overall by examining the capability of its member organizations.

The C2M2 is meant to be used by an organization to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. An organization performs an evaluation against the model, uses that evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated.

To measure progression, maturity models typically have “levels” along a scale—C2M2 uses a scale of maturity indicator levels (MILs) 0–3, which are described in Section **Error! Reference source not found.**. A set of attributes defines each level. If an organization demonstrates these attributes, it has achieved both that level and the

capabilities that the level represents. Having measurable transition states between the levels enables an organization to use the scale to:

- Define its current state
- Determine its future, more mature state
- Identify the capabilities it must attain to reach that future state

The model arises from a combination of existing cybersecurity standards, frameworks, programs, and initiatives. The model provides flexible guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the model practices tend to be at a high level of abstraction, so that they can be interpreted for organizations of various structures and sizes.

The model is organized into 10 domains. Each domain is a logical grouping of cybersecurity practices. The practices within a domain are grouped by objective—target achievements that support the domain. Within each objective, the practices are ordered by MIL.

The C2M2 Version 2.0 initiative leverages and builds upon existing efforts, models, and cybersecurity best practices to advance the model by adjusting to new technologies, practices, and environmental factors that have occurred since the Version 1.1 release.

Advances between C2M2 Versions 1.1 to 2.0

The C2M2 Version 2.0 was necessitated by advancements in technologies, practices, and frameworks to protect critical infrastructure against cyber intrusions. A comprehensive review of all domains and MILs conducted by teams of industry experts ensured C2M2

Version 1.1 user concerns were addressed and revisions to domains and MILs were achieved in accordance with user feedback. C2M2 Version 2.0 builds upon initial development activities and was further developed through the following approach:

Public–private partnership: Numerous government, industry, and academic organizations participated in the development of this model, bringing a broad range of knowledge, skills, and experience to the team. The model was developed collaboratively with an industry advisory group through a series of working sessions, and it was revised based on feedback from more than 60 industry experts with extensive experience using Version 1.1.

Best practices and sector alignment: The model builds upon and ties together a number of existing cybersecurity resources and initiatives and was informed by a review of cyber threats to the energy sector. Leveraging related works shortened the development schedule and helped to ensure that the model would be relevant and beneficial to the sector.

Descriptive, not prescriptive: This model was developed to provide descriptive, not prescriptive, guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the model practices tend to be abstract so that they can be interpreted for entities of various structures, functions, and sizes.

Fast-paced development: The development effort focused on quickly developing a model that would provide value to the energy sector and be available as soon as possible. The sector has widely adopted the model and provided valuable feedback for improvements.

The model has also been enhanced to account for updates made to the NIST Cybersecurity Framework. While aligning with the NIST Framework and accounting for Version 1.1 comments, the development of Version 2.0 updates include the following:

- Establishing a Cybersecurity Architecture domain
- Separating the MILs from the Information Sharing and Communications domain to include sharing practices in the Threat and Vulnerability Management and Situational Awareness domains
- Movement of Continuity of Operations MILs from the Incident and Event Response to the Cybersecurity Program Management domain to account for continuity activities beyond response events
- Increasing the use of common language throughout the model

A mapping of C2M2 Version 1.1 to 2.0 will be included in Appendix B in the final document to ensure existing users can understand variations from historical evaluation scoring to continue the maturation process with the changes to the model.

Signed in Washington, DC on August xx, 2019

_____

Timothy Kocher
Special Advisor
Office of Cybersecurity, Energy Security, & Emergency Response
U.S. Department of Energy