This material is based upon work funded and supported by the Department of Energy under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0831

2 Meeting Overview

The U.S. Department of Energy (DOE) hosted a Cybersecurity Capability Maturity Model (C2M2) Working Group (WG) meeting May 23, 2018, at its Washington D.C. headquarters. The Software Engineering Institute (SEI) co-organized and hosted the half-day event. The purpose of the WG meeting was to work through issues identified in the previous day's C2M2 Stakeholder Forum.

WG participants in the meeting included

- Laura Brown, E-ISAC
- Fowad Muneer, U.S. Department of Energy
- Mike Isper, U.S. Department of Homeland Security/TSA
- Jim Linn, American Gas Association
- Kegan Gerard, American Gas Association
- Nathan Mitchell, American Public Power Association
- Tamara Lance, Atmos Energy
- David White, Axio
- Brendan Fitzpatrick, Axio
- Kristen Quade, E-ISAC
- John Fry, Ernst & Young
- Samara Moore, Exelon
- Linda Conrad, Exelon
- Moin Shaikh, ICF (DOE affiliate)
- Annabelle Lee, Nevermore Security
- Matthew Barrett, NIST
- Julia Mullaney, Software Engineering Institute
- Alexander Petrilli, Software Engineering Institute
- Paul Ruggiero, Software Engineering Institute
- Jeffrey Pinckard, Software Engineering Institute
- Brian Benestilli, Software Engineering Institute
- Matthew Trevors, Software Engineering Institute
- Michael Rattigan, Software Engineering Institute
- Charles M. Wallen, Software Engineering Institute
- Jason Tugman, Southern Company
- Chris Taylor, Southern Company
- Dan Lagraffe, U.S. Department of Energy
- Stephen Abott, ICF (DOE affiliate)
- Walter Grudzinski, Vectren

The meeting consisted of a summary of the Stakeholder Forum's outcomes, a working session about those outcomes, and a working session on the C2M2 v2.0 survey.

This report summarizes the WG meeting's activities and documents its outcomes.

3 Meeting Summary

3.1 Strategy Session

The conversation began with the meaning of resilience management, which led to the suggestion that the model use the term "operational risk management," which will resonate more with OT personnel and the industry in general. However, using that term risks undervaluing resilience management and pigeonholing it within operations. It was decided to table the discussion and take an action to better define "resilience management."

The next topic was scoping. Scoping to a function matters and impacts what is considered operational. However, the C2M2 should already be focused on a given function, so perhaps the focus should be on soliciting suggestions for a new name.

Tailoring the model was a theme from the previous day's stakeholder forum. Version 2.0 of the model should continue to enable tailoring for different roles and responsibilities.

Reinforcing the C2M2's CERT-RMM heritage, or adding guidance that points back to CERT-RMM, could backfire. Smaller organizations might see the connection as a barrier to entry. Though the CERT-RMM is an important part of C2M2, it does not serve the needs of the energy sector, which resisted deriving their cybersecurity maturity model from CERT-RMM. Reinforcing the connection now risks alienating the community. That said, MILs 4 and 5 might be a useful point of entry for CERT-RMM.

The next topic was community engagement with the development of C2M2 v1.0, v1.1, and v2.0. The original version of the model had credibility within the sector because community members were deeply involved in its development and felt ownership over it. Community involvement in the v2.0 development should be robust and carefully communicated. The community must once again feel a sense of ownership. It was agreed that the Working Group would give the associations time to build consensus among their members.

The next topic was how the Working Group should function. The Working Group and Sub-Working Group meetings were seen as unfocused and one-sided. The SEI's role and expertise was debated. It was agreed that the SEI will make the commenting, adjudication, and feedback processes more transparent. It was also agreed that the initial deadline for v2.0 development was flexible, and that it was better to extend the deadline in favor of a more complete end product.

The Working Group discussed the best way to get industry feedback on v2.0 development. The straw man sent by DOE to the Federal Register did not solicit sufficient feedback, so the effort is pivoting to the survey. However, it was suggested that a second, updated strawman be put forth.

3.2 Survey

The goal of the survey was to communicate to the SCCs the key requirements for v2.0 and solicit their thoughts on risk guidance. It was decided to modify the demographics questions to expand the response options for the respondent's role.

The group debated how to define alignment to other standards and frameworks. It was agreed that v2.0 should map to NIST CSF, but the way the mapping is referred to should not trap C2M2 into a one-to-one alignment with CSF or any other standard.

The questions about the length of the assessment were debated and edited.

The group expressed trepidation about adding the ability to de-scope the model. Instead, the model might have staged scoping as an on-ramp.

The group discussed whether or not the survey should ask about the need for a report presentation or template to be included in the toolkit.

The group also discussed how the survey should address adding a business continuity domain.