

Abstract Submission
for
TENTH ANNUAL CARNEGIE MELLON CONFERENCE ON THE ELECTRICITY INDUSTRY

Title:

Evaluating and Improving Cybersecurity Capabilities of the Electricity Critical Infrastructure

Authors:

Pamela Curtis, Dr. Nader Mehravari, and Katie Stewart
Cyber Risk and Resilience Management Team
Software Engineering Institute (SEI)
Carnegie Mellon University

Corresponding Author:

Dr. Nader Mehravari
Email: nmehravari@sei.cmu.edu
Mobile: 607-379-9556

Abstract:

This paper describes the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). It is a proven tool which allow owners and operators of components of electricity critical infrastructure to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity. It combines elements from existing cybersecurity efforts into a common tool that can be used consistently across the industry. The ES-C2M2 was developed 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 electricity subsector as well as from industry, private sector, public sector, and other stakeholders. The model was developed to apply to all electric utilities, regardless of ownership structure, size, or function. Broad use of the model is expected to support benchmarking for the subsector's cybersecurity capabilities. The goal of these models and associated tools are to support ongoing development and measurement of cybersecurity capabilities within the electricity and oil and natural gas subsectors through the following four objectives: (1) Strengthen cybersecurity capabilities in the subsector, (2) Enable subsector entities to effectively and consistently evaluate and benchmark cybersecurity capabilities, (3) Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities, and (4) Enable subsector entities to prioritize actions and investments to improve cybersecurity. In this presentation we will provide background on the ES-C2M2, including the model architecture, an overview of the domains, and the model practices. We will explain the Cybersecurity Self Evaluation Survey Tool, which helps electric utilities and grid operators use the model to identify opportunities to further develop their own cybersecurity capabilities. In addition, we will describe the development of the Oil & Natural Gas variant of the model (ONG-C2M2). Finally, we will share information about how these models have successfully been utilized by an ever increasing number of entities and plans for their continued stewardship, evolution, and applications to other types of organizations.