Operational Technology Cybersecurity Coalition

November 6, 2023

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899-2000
Email: cyberframework@nist.gov

Re: Operational Technology Cybersecurity Coalition Support for NIST CSF 2.0

Thank you for the work that the National Institute of Standards and Technology (NIST) has put into its multi-year effort to update the NIST Cybersecurity Framework (CSF or Framework) 2.0; especially as it applies to operational technology. The Operational Technology Cybersecurity Coalition (OTCC) is a diverse group of leading industrial control systems (ICS) and operational technology (OT) cybersecurity vendors covering the entire OT lifecycle. As such, we strongly support the draft NIST Cybersecurity Framework 2.0 (CSF 2.0) that was released on August 8, 2023.

OT cybersecurity endeavors to prevent attacks targeting industrial and process control equipment along with IoT technologies. The proliferation of known product vulnerabilities in OT systems necessitates a robust framework like CSF 2.0 to accurately contextualize risks to industrial environments based on specific products, services, resources, processes, and technologies.

CSF 2.0's alignment with relevant NIST resources allows practitioners to manage enterprise risk in a holistic manner. These include the NIST Privacy Framework; NICE Workforce Framework for Cybersecurity (SP 800-181); Secure Software Development Framework (SP 800- 218); Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161r1); Performance Measurement Guide for Information Security (SP 800-55); Integrating Cybersecurity and Enterprise Risk Management (NIST IR 8286) series; and the Artificial Intelligence Risk Management Framework (AI 100-1).

CSF 2.0 makes a statement in lines 138-140 that indicates the framework is intended to cover all Information Technology (IT), Internet of Things (IoT), and notably, Operational Technology (OT) utilized by an organization. However, we have some concerns that the simple reference to CSF 2.0's application to OT and IoT makes the same mistake we see all too often in our field; it leaves the impression that processes undertaken to secure IT can simply be applied to OT and IoT. This isn't true.

In applying cybersecurity frameworks to IT versus OT environments, they require slightly different approaches. We therefore recommend that in lines 138-140, that distinction should be made and that users of CSF 2.0 be directed to seek additional OT guidance from NIST's OT-specific resources.

In cases where there is a difference in approach to IT and OT cybersecurity implementations NIST should provide guidance by leveraging NIST resources including guidance documents and implementation examples. We therefore encourage NIST to reference OT-specific resources such as the recently updated NIST Special Publication SP 800-82r3, Guide to Operational Technology (OT) Security in both the newly developed Reference Tool, and the National Online Informative References, or OLIR. Further, as the

Reference Tool is new, we hope that there will be a public comment period for the Reference Tool before the document is finalized.

We also recommend the inclusion of the Idaho National Laboratory's work on Cyber-Informed Engineering (CIE) and Consequence-Driven CIE (CCE) in both the Reference Tool and OLIR. These frameworks aim to guide the application of cybersecurity principles across the engineering design life cycle, and "engineer out" potential risk in key areas within the design of engineered systems.

Advancements made in CSF 2.0 are foundational to meeting the cyber requirements in the U.S. National Cybersecurity Strategy, and underscores the necessity for a modern, agile regulatory frameworks tailored to each sector's risk profile, thereby reducing duplication, fostering public-private collaboration, and being mindful of implementation costs and resource strains. As this and future administrations work to develop global cybersecurity standards, we view CSF 2.0 as a resource to drive those negotiations.

Finally, the provision of Implementation Examples is an incredibly helpful tool to provide organizations without deep expertise or resources useful case studies to help them achieve the framework's desired outcomes. However, we encourage NIST to ensure that the Implementation Examples provide clear guidance to effectively help small to medium sized critical infrastructure owners and operators implement the framework.

Again, the OTCC appreciates the work that has gone into this draft CSF 2.0, and the open, collaborative process undertaken by NIST.

Sincerely,

Andrew Howell

Andrew Howell
Executive Director, OTCC
[redacted]