Comments on Draft 2 of NIST Cybersecurity Framework 1.1

Feedback and comments are directed to cyberframework@nist.gov.

To whom it may concern;

Please accept the following comments as part of the review of the latest edition of the NIST Cybersecurity Framework. Any questions about this feedback may be directed to:

Eric C. Cosman

OIT Concepts, LLC
eric.cosman@oitconcepts.com
Co-Chair, ISA99 committee in industrial automation and control systems security

Responses to Questions Posed

1. Do the revisions in Version 1.1 Draft 2 reflect the changes in the current cybersecurity ecosystem (threats, vulnerabilities, risks, practices, technological approaches), including those developments in the Roadmap items?

    Inclusion of more information about risk assessment (Section 4.0) is a welcome addition to the Framework.

2. For those using Version 1.0, would the proposed changes affect their current use of the Framework? If so, how?

    Yes, I believe so. It has been some time since I have been directly involved in an application of the Framework, but based on my experience, the usefulness is definitely increasing with each revision.

3. For those not currently using Version 1.0, would the proposed changes affect their decision about using the Framework? If so, how?

    See above comment.

Detailed Comments

Line 119, page 2

"As the Framework is put into greater practice, additional lessons learned will be integrated into future versions."

Are there plans to develop some sort of collection of use cases or case studies that illustrate specific "lessons learned" through implementation?

Line 171, page 4:

"The Framework remains effective and support[s] technical innovation, because it is technology neutral, …"

Line 351, page 9 (Framework Implementation Tiers)

The tier concepts presented in this Framework is similar to the maturity model concept presented in the ISA-62443 / IEC 62443 and similar standards. It may be a worthwhile exercise to conduct a more detailed comparison of the two.

I would also encourage a review of the "protection level" concept currently being developed by the ISA99 committee for inclusion in the ISA-62443 / IEC 62443 standards. More information is available in the form of a draft technical report:

"Security for industrial automation and control systems – Part 1-5: Industrial automation and control system protection levels"

Section 3.2, page 15 (Establishing or Improving a Cybersecurity Program)

This section outlines a seven-step approach for program implementation. Consider the addition of an eight step, focused on the creation of a “control plan” or outline of what is required to sustain performance.

Line 640, page 17

In this paragraph describing figure 3, where do cybersecurity services fit? Should they be considered as “technology”, or “not technology?”