PUBLIC SUBMISSION

As of: 4/25/22 12:18 PM
Received: April 15, 2022
Status: Pending_Post
Tracking No. l20-qbkh-xzua
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0019
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Xcel Energy, Inc.

General Comment

See attached file(s)

Attachments

Xcel Energy Response to RFI-2022-03642

Response to RFI-2022-03642

This document contains a response to NIST's Request for Information (RFI) to provide feedback on the cybersecurity framework (CSF). A team of Security Risk Analysts and Cyber Security Engineers employed at Xcel Energy have been gathering information (or data) since mid-2021 to better understand the NIST CSF and its application to our business partners, to conduct effective Security Risk Assessments. We have compiled the following notes resulting from that effort and, have organized what we consider to be most important comments to those of least importance to address.

Definitions in italics within parentheses are from NIST's Glossary at https://csrc.nist.gov/glossary/

CHANGES PURELY TO THE CSF ITSELF

1. Each subcategory could benefit from examples, including controls that could be used.
2. Each subcategory could provide guidance on ties to Operational Technology (OT) as not all may apply. It may warrant a separate CSF.
3. ID.AM-1 and ID.AM-2 refer to an inventory (*A listing of items including identification and location information.*), while ID.AM-4 refers to a catalog (*The collection of all assessment elements.*). How do these differ, or do the terms have the same definition within the CSF?
4. RS.MI-3 could potentially be incorrect, and it would depend on the definitions of *mitigation* (*A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities.*) and *remediation* (*The act of mitigating a vulnerability or a threat.*).
    a. Xcel Energy defines *remediation* as a full elimination of security risk, while *mitigation* indicates a lessened impact or likelihood of the occurrence of security risk.
    b. This subcategory indicates two paths for a newly identified vulnerability: a risk can be accepted, or it can be *mitigated*. If mitigation does not mean the risk is removed, this implies that the risk acceptance could be avoided if impact or likelihood is merely lessened.
    c. Xcel Energy requires risk to be *remediated* or the risk must be accepted. We would recommend changing the subcategory to read: Newly identified vulnerabilities are remediated or documented as accepted risks.
5. Many subcategories refer to events (*Any observable occurrence in a system*.), while others refer to incidents (*An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies*.). Can clarity about the relationship between the two terms be provided, unless the CSF considers them to mean the same thing? The Glossary has many definitions of *incident* and that could be clarified.
6. A few subcategories suggest stakeholders *understand* their roles and responsibilities, like PR.AT-2. RS.CO-1 suggest stakeholders must *know* roles. Xcel Energy's required training *informs* users, but an audit, quiz, or interview would be needed to ensure users *understand* or *know* roles and responsibilities. Is this the spirit of these subcategories, or should the guidance be only to *inform*? Is there a difference between *understanding* and *knowing* in this context? These terms may benefit from definitions in the Glossary.
7. PR.DS-8 references hardware integrity. Other than tamper tape on assets provided by vendors, what is the NIST expectation? Are administrators expected to regularly examine circuit boards to identify unauthorized hardware changes? As this would void warranties and require specialized knowledge, this will likely not occur. What are the NIST expectations?

8. PR.IP-7 refers to continuous improvement of protection processes. This is an important call-out, and one that is lacking for other processes referenced in the CSF. Should there be a more general subcategory noting that all processes should be continuously improved, or can these specific subcategories be added in other sections?
9. DE.CM-4 indicates malicious code should be detected, but should it also indicate actions to be taken if it is detected?
10. DE.CM-5 indicates unauthorized mobile code should be detected, but should it also indicate actions to be taken if it is detected?
11. Could DE.CM-5 be more general to refer to **any** unauthorized code rather than focusing solely on mobile code?
12. DE.DP-2 could be refined. It seems to indicate that detection activities must follow requirements, which could be set for all activities in the CSF. It may not need to be mentioned at all. A possible rewording could be: Detection activities must have applicable requirements documented and implemented.
13. RS.CO-2 could also require the criteria it mentions to be identified and documented.
14. ID.BE-4 has a few terms that could change the spirit of the subcategory depending on how they are defined.
    a. How does NIST define *critical* for functions and services? If it is up to each organization to define it, some guidelines and recommendations would be helpful.
    b. The terms *functions* and *services* may not be terms used at all organizations. Some guidance would be helpful.
15. We would recommend moving PR.IP-9 and PR-IP-10 to the Response and Recovery sections, as that is what they refer to. When working with internal stakeholders on understanding Implementation Levels, these two subcategories would require Business Continuity where the others in the Protect section may not. Can they be moved?
16. PR.IP-11 implies many controls, and it may benefit from being split into multiple subcategories.

ALIGNMENT BETWEEN THE CSF AND OTHER NIST RESOURCES

How can we align the CSF with OT guidance, specifically 800-82 rev2? It is not clear.

WAYS TO IMPROVE CYBERSECURITY IN SUPPLY CHAINS

Supply chain should be manifested in additional places within the CSF; i.e., rather than just in the 'Identify' function, as now, to within the 'Respond' and 'Recover' functions as well.

There are many variables present in the 'Identify' function of supply chain security risk activities and approaches that can negatively impact the overall security posture of a vendor arrangement. Many of these are reasonable from a business perspective, given the multitude of risk considerations (including but beyond security) that entities consider when engaging a supplier for cyber-related products and services. For instance, for valid business reasons management often decides to accept some portion of security risk when it proceeds to initiate vendor arrangements.

But we've seen that there are unique security risk challenges of supplier arrangements *post implementation*, when a notable vendor product vulnerability is identified, when security incidents occur at vendor entities that have downstream impacts on customer entities, etc. There's no difficulty of management wishing to 'accept' inactivity in response to such matters (which is good), but there are unique challenges in how to identify and implement optimal responsive approaches. The 'Respond' and 'Recover' activities associated with such situations are somewhat unique for customer entities relying on an affected third-party, due to the very nature of the relationship (reliance on the third-party for timely information that something is amiss, and specifics about how best to respond), and to date such activities have proven to be a struggle for many customer entities (log4j, SolarWinds, etc.).