NIST Cybersecurity RFI
Contact: Carol Muehrcke
ISA Global Cybersecurity Alliance (ISAGCA)
April 25, 2022

Introduction

The following comments are in response to the NIST Cybersecurity RFI published Feb 22, 2022.

- **Presentation of informative references in general and of 62443 in particular:** In response to the NIST Cybersecurity Framework topic described in the supplementary information provided with that RFI:
  "Any features of the NIST Cybersecurity Framework that should be changed, added, or removed…. These might include additions or modifications of … references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework"

  - The NIST CSF v1.1 mapping presentation in Table 2 places practical limits on the number of references to other documents, since the subcategory and requirement-level detail shown is lengthy, and also subject to ongoing maintenance, as the references themselves evolve.
  - A practical approach for offering external references by subcategory would be to remove the subcategory-level mapping information, and instead create a separate section of the NIST CSF document that lists titles of example reference documents, and describes the scope of each reference document at a high level. Each of these reference documents then could have a corresponding detailed mapping spreadsheet posted on the NIST OLIR (Online Informative Reference) website. The NIST CSF document would provide a general pointer to that site. Either NIST or another party could create these OLIR spreadsheets for the existing external references in NIST CSF v1.1, and for other external references.
  - This gives the opportunity for NIST CSF to incorporate more references, and to provide a helpful categorization of references listed in the NIST CSF by general topic area or keywords (such as risk management, industrial control systems). For example, although NIST CSF includes several mentions of industrial control systems and their distinctive characteristics, there is not an explicit statement that the 62443 series addresses this domain. Further, making the OLIR program the primary vehicle via which to provide NIST CSF references also encourages other organizations to provide such mappings.
  - The current NIST CSF v1.1 contains in Table 2, references to ANSI/ISA 62443-3-3 *System security requirements and security levels*, and ANSI/ISA 62443-2-1 *Security program requirements for IACS asset owners*. The revised approach outlined above will give the opportunity to provide references for all parts of the 62443 standard and related reports, including ANSI/ISA 62443-2-4 *Security program requirements for IACS service providers*, ANSI/ISA 62443-3-2 *Security risk assessment for system design*, and ANSI/ISA 62443-2-3 *Patch management in the IACS environm*ent.
  - ISAGCA is currently working on creating submissions to the NIST OLIR program for ANSI/ISA 62443-3-3 and for ANSI/ISA 62443-2-1. The latter is being done in conjunction with an update of the ANSI/ISA 62443-2-1 standard, which will replace the currently published version now referenced by NIST CSF v1.1.

- **Challenges with framing:** The core structure and content are found very helpful and intuitive. Challenges in using the document lie with the surrounding framing about how to use the core. This framing material is difficult to follow, in part because the document attempts not to prescribe or limit how the core could be used. That said, we fully agree with being non-prescriptive. The framing challenge is then to help readers build a clear picture of how the core might be used, without prescribing how to use it, for an audience coming in schooled in a wide variety of cybersecurity management approaches and standards. The comments below are intended as a contribution toward achieving that goal.
- **"Levels" of security:** A number of cybersecurity approaches incorporate concepts that define levels of security, for example, low, moderate, and high impact systems in FIPS 200, and capability security levels 1-4 in 62443. It would be helpful to state how this general concept relates to the use of the framework. It appears that a "level" concept of this type may be used as a method to select outcomes and implementations for outcomes. Possibly outcomes are sufficiently abstract so that many differences by "level" of security will be found only in selection of implementation. The framework likely does not intend to lay out a specific method to be used to create a profile or select implementations to achieve those outcomes in the profile (other than that it be based upon a risk assessment). Clarifying this point about what the framework does NOT intend to do, would make it clearer how to use the CSF together with other standards and guidelines that do intend to do those things. See related comment "From risk to selection of implementations."
- **Content of profile:** While it is clear that a profile requires selecting a subset of the CSF outcomes, it could be made clearer what further content, if any, defines a profile. Does a profile include specific requirements from referenced standards? Does it include intended implementations of those requirements? Are these the contents intended in the statement: "The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario?" A partial example of a profile covering one or two subcategories would be helpful.
- **From risk to selection of implementations:** The CSF states that risk assessment informs selection of subcategories and implementations of those subcategories in the informative references. Although it appears the CSF does not intend to specify this step in detail, it could be helpful to acknowledge that this flexibility is intentional, and provide illustrative examples of how this step could be carried out based upon various risk assessment methods. One example is that as a step in risk assessment, 62443-3-2 requires creation of security zones, and assignment of a target security level to each of those zones. Four security levels are defined by the standard. 62443-3-3 then defines functional capabilities to be implemented to support each security level.
- **Heterogeneity:** From CSF 2.3 page 11: *"Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs."* It is noted that the issue may not be complexity. Instead, one can replace "complexity" by "heterogeneity." Organizations include functions that are usually heterogeneous in terms of security requirements, such as marketing vs. human resources vs. accounting vs. refinery control vs. refinery safety functions. It will affect cost, effectiveness, ease of management and risk to make the right decisions about what should be common in these profiles and their implementations, and what

should be different. In addition to the functional dimension, another dimension of heterogeneity is temporal. For example, the level of security required for an industrial control system may be different (in electricity generation) when fueling, starting the turbines, or performing remote maintenance to change logic on the controllers.

- **Clarify how distinction between IT and CS, ICS, and IoT devices affects use of framework:** From CSF Appendix A p22: "*Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.''* It would be helpful to say more explicitly that these considerations will affect the selected outcomes and means of achieving the outcomes selected, when creating the profile(s) for these types of systems. An example such as the following could be useful. Related to the sub category DE.CM-8 *Vulnerability scans are performed*, a particular solution selected to comply with a related reference for IT systems, may cause unacceptable performance degradation on an OT system, leading to process anomalies that create a safety hazard.
- **Tiers:** A number of ISAGCA stakeholders reported that they are using the core aspect of the framework, and are not using the concept of tier. Clarifications of the intended audience for the tier concept, as well as the concept itself, are offered here.

  In terms of audience, the organizational levels that could influence a tier, are typically higher than those that use the core part of CSF to organize their efforts. A cybersecurity analyst using the core at the Business/Process level in Figure 2 would typically respond to, but not recommend or make decisions about having an organization-wide risk management policy or interactions with the organization's supply chain or community, which are example elements in the tier definitions. Figure 2 about organization information and decision flows, is accurately titled as "*Notional*." It could be clarified further that based upon unique organizational structures, different organizational functions or levels may employ tiers, or the core, as driving concepts.

  In terms of concept definition, the document states "*Tiers do not represent maturity levels.*" It would seem then, from the following text in the CSF 2.2, that a tier is a security level.

  > *Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs)…*

  However, the tier definitions do not imply that higher levels of security are achieved at higher tiers. They do imply that more appropriate levels of security are achieved at higher tiers. The level of security implemented might in fact become lower as the organization better understands and accepts their risk. In summary, the tier concept may be a useful management tool (though neither a maturity level nor a security level), but its logical connection and position as a key concept in the

framework is not well explained. Becoming skilled at finding the appropriate level of risk is about skill at risk management, which the framework states is a topic outside of its scope and covered by a number of other documents, as the framework "*can be used with a broad array of cybersecurity risk management processes*." The major point could be explicitly made, that since the use of the core is to be based on risk management, an organization will benefit from having a way of gauging its skill at cybersecurity risk management, separately from the risk management method selected. Tiers could then be given as an example of a method for gauging this. It could also be clarified whether there is one tier, or one per category, or subcategory, or whether this is flexible for the needs of the organization.