PUBLIC SUBMISSION

As of: 4/27/22 6:37 AM
Received: April 25, 2022
Status: Pending_Post
Tracking No. l2f-075r-vggp
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-0045
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Santander Bank

General Comment

This is a great initiative. Please see comments from Santander Bank (more details in the document attached)
1. NIST CSF Implementation Tiers are challenging to use due to the non-specificity relating to each CSF category. This includes both initial assessment and development of a roadmap for on-going maturity. As a result, alternative frameworks may be used e.g., the FFIEC CAT. Further challenge is created when the Organization is looking to move to a more mature framework such as the NIST 800.53 with limited guidance on how these requirements should be looked at from an on-going maturity/maturity roadmap stand-point, and the interaction between the NIST CSF and NIST 800.53.
We consider that developing additional guidelines to implement the sub-categories (similar to the "Supplemental Guidance" of NIST 800-53 controls) would be valuable, as well as more guidance with a proposed set of indicators for each category/sub-category to assess the implementation and effectiveness of the requirements.
In regards to the "Supplemental Guidance" for each CSF sub-category, it would be also beneficial to have the specific guides published by NIST (Ransomware, BYOD, etc.) mapped with each sub-category, similar to the existing mapping with other frameworks and standards (NIST SP 800-53, ISO/IEC 27001, COBIT 5, etc.).
2. NIST CSF is widely adaptable to most organizations and industries, however additional sector specific sets of sub-categories by critical infrastructure sectors could be recommended (e.g. Financial Services, Health, Energy, etc.).
3. While the NIST CSF is a comprehensive framework (with near 100 sub-categories) and can form a strong basis for Organizations to establish requirements and secure their systems, the NIST Risk Management Framework is intended to be used as a reference model for establishing the risk profile of an Organization with a limited scope (systems). Mapping CSF categories/sub-categories with references to existing (and recognized) risk management models could be recommended to facilitate performing risk assessment and measure the risk level of an Organization.
4. New Topics for CSF: The following emerging topics are considered for inclusion in the NIST CSF or

other supplementary guidance.
a. Cloud Category
b. DevSecOps
5. Reviewing the current sub-categories of the CSF Framework, certain upgrades could be considered:
a. Access Control (PR.AC):
A specific sub-category for the periodic review of accesses is missing (Recertification process).
b. Respond Improvements (RS.IM):
A specific sub-category for the testing of response plans is missing.
c. Awareness and Training (PR. AT):
Specific sub-categories for the periodical evaluation of cybersecurity awareness education and training campaigns is missing. Also consider the inclusion of consequence management requirements for users who repeatedly/intentionally fail completing training & awareness program and/or complying with security policies.
d. Information Protection Processes and Procedures (PR.IP) which is a catch all bucket for several independent topics/functions. It would be useful to split out and expand some topics covered in this section.
¯ Build out of ID.BE-5 (Resiliency Requirements)
¯ Build out of PR.IP-3 (Configuration Change Control)
¯ Build out of PR.IP-2 (SDLC)
e. Expansion of PR.PT (Protective Technology)
There is potential to expand this section to cover the specific protective controls an organization should consider implementing to ensure adequate coverage of "Communications and Control Networks" (PR.PT-4) without being overly prescriptive in the controls that must be applied (e.g. email/spam protections and network boundary protections).
Supply Chain Category:
¯ Given the relevance of the supply chain processes, it might be appropriate to focus and include some specific Supply Chain sub-categories aligned with the principles of NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations ". The current CSF has a narrow view of what is considered a supply chain attack. Current requirements are challenging to assess/implement applicability to the Financial Services Industry:
o Suggestion to re-define what is meant be a Supply Chain Attack to consider an organization using the CSF and re-work the associated requirements in the CSF:
Dependency on a vendor (Consumer)
AND / OR
Providing critical services to another organization (Provider/Supplier)
¯ Consideration to re-name section ID.SC (Supply Chain Risk Management) to Third Party Risk Management in line with other Industry frameworks.
Requirements to include/expand upon: Definition of the value/supply chain -> Identification of Risk (ID.SC-2:) --> Identification of controls --> Implementation of common controls.

Attachments

Open Request NIST-2022-0001 - Santander

Review of NIST Open request NIST-2022-0001

1. **NIST CSF Implementation Tiers** are challenging to use due to the non-specificity relating to each CSF category. This includes both initial assessment and development of a roadmap for on-going maturity. As a result, alternative frameworks may be used e.g., the FFIEC CAT. Further challenge is created when the Organization is looking **to move to a more mature framework** such as the NIST 800.53 with limited guidance on how these requirements should be looked at from an on-going maturity/maturity roadmap stand-point, and the interaction between the NIST CSF and NIST 800.53.

   We consider that **developing additional guidelines to implement the sub-categories** (similar to the "Supplemental Guidance" of NIST 800-53 controls) would be valuable, as well as more **guidance** with a proposed set of indicators for each category/sub-category **to assess the implementation and effectiveness of the requirements**.

   In regards to the "Supplemental Guidance" for each CSF sub-category, it would be also beneficial to have the **specific guides published by NIST** (Ransomware, BYOD, etc.) mapped with each sub-category, similar to the existing mapping with other frameworks and standards (NIST SP 800-53, ISO/IEC 27001, COBIT 5, etc.).

2. NIST CSF is widely adaptable to most organizations and industries, however **additional** sector specific **sets of sub-categories by critical infrastructure sectors** could be recommended (e.g. Financial Services, Health, Energy, etc.).

3. While the NIST CSF is a comprehensive framework (with near 100 sub-categories) and can form a strong basis for Organizations to establish requirements and secure their systems, the NIST Risk Management Framework is intended to be used as a reference model for establishing the risk profile of an Organization with a limited scope (systems). Mapping CSF categories/sub-categories with references to existing (and recognized) risk management models could be recommended to facilitate performing risk assessment and measure the risk level of an Organization.

4. **New Topics for CSF**: The following emerging topics are considered for inclusion in the NIST CSF or other supplementary guidance.

   a. Cloud Category:
      Alignment to the Cloud International standards should be considered (i.e. Cloud Security Alliance (CSA) framework and CIS Controls Cloud Companion Guide). Develop an up-to-date approach to Cloud environments focusing in shared responsibilities within the Supply Chain and modern cloud security practices (configuration, connectivity, virtual infrastructure and security, automation, etc.).

   b. DevSecOps:

There are many best practices available such as SAMM, BSIMM, OWASP, and SAFECode for security development process. However, there is no clear benchmark. DevSecOps framework should provide guidelines for establishing an application security champion program and for automating security processes (i.e. threat modeling, integrating threats with testing such as SAST, DAST and Pentest, etc.).

5. Reviewing the current sub-categories of the CSF Framework, **certain upgrades could be considered**:

   a. Access Control (PR.AC):
   A specific sub-category for the periodic review of accesses is missing (Recertification process).

   b. Respond Improvements (RS.IM):
   A specific sub-category for the testing of response plans is missing.

   c. Awareness and Training (PR. AT):
   Specific sub-categories for the periodical evaluation of cybersecurity awareness education and training campaigns is missing. Also consider the inclusion of consequence management requirements for users who repeatedly/intentionally fail completing training & awareness program and/or complying with security policies.

   d. Information Protection Processes and Procedures (PR.IP) which is a catch all bucket for several independent topics/functions. It would be useful to split out and expand some topics covered in this section.
      - Build out of ID.BE-5 (Resiliency Requirements) to cover the implementation of resiliency requirements, e.g. BIA. This could include re-arranging these requirements along with PR.IP-9 and 10 into its own category.
      - Build out of PR.IP-3 (Configuration Change Control) to cover more holistically Change Management - covering the requirement to establish effective change management processes (outside of just configuration). This could include splitting "Change Management" out of PR.IP into its own category.
      - Build out of PR.IP-2 (SDLC) to cover additional requirements for secure SDLC. This may include establishment of security architecture requirements, security testing and project management processes which ensure all software/systems/projects are adequately reviewed for information security risk prior to introduction into an environment.

   e. Expansion of PR.PT (Protective Technology)

There is potential to expand this section to cover the specific protective controls an organization should consider implementing to ensure adequate coverage of "Communications and Control Networks" (PR.PT-4) without being overly prescriptive in the controls that must be applied (e.g. email/spam protections and network boundary protections).

Supply Chain Category:

- Given the relevance of the supply chain processes, it might be appropriate to focus and include some specific Supply Chain sub-categories aligned with the principles of NIST SP 800-161 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations ". The current CSF has a narrow view of what is considered a supply chain attack. Current requirements are challenging to assess/implement applicability to the Financial Services Industry:
  - Suggestion to re-define what is meant be a Supply Chain Attack to consider an organization using the CSF and re-work the associated requirements in the CSF:
    - Dependency on a vendor (Consumer)
      AND / OR
    - Providing critical services to another organization (Provider/Supplier)

- Consideration to re-name section ID.SC (Supply Chain Risk Management) to Third Party Risk Management in line with other Industry frameworks.

  Requirements to include/expand upon: Definition of the value/supply chain -> Identification of Risk (ID.SC-2:) --> Identification of controls --> Implementation of common controls