April 25, 2022

Submitted via email to: CSF-SCRM-RFI@nist.gov

National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
Subject: *NIST-2022-001 / Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*

Accenture appreciates the opportunity to share comments and recommendations regarding the National Institute of Standards and Technology's (NIST) efforts to update its Cybersecurity Framework (CSF). NIST has continually demonstrated its commitment to engaging in a transparent and collaborative process with industry, and this process has been no different.

Accenture Security has approximately 16,000 security professionals across our advanced cyber defense, applied cybersecurity solutions, managed security, and industry solutions services. We help businesses identify, protect, detect, respond, and recover along all points of the security lifecycle. Leveraging our global resources and next-generation technologies, we create integrated, practical solutions that are tailored to each organization's specific business goals and industry. We serve more than 1,700 critical infrastructure clients in the U.S. alone. Whether defending against known threats, quickly detecting and responding to the unknown, or running an entire security operations center, we help harden these organizations and make it extremely difficult for even the most sophisticated cyber adversaries to succeed.

As part of our services, we provide independent cybersecurity program assessments, including utilizing NIST's CSF to examine an organization's threat-based targets and profiles and scoring across functions, categories and subcategories. Accenture as an enterprise also aligns its risk assessment with the CSF, along with other security controls and assessments.

Relying on our experience performing NIST CSF assessments and our expertise helping organizations assess risk and protect their most important assets, we have made both general framework comments in response to NIST's questions, and specific recommendations about individual categories and subcategories for NIST's consideration. To that end, we have included the general framework feedback below, and are also submitting a spreadsheet with the detailed recommendations and analysis for each of the CSF functions, categories and subcategories.

Accenture Security looks forward to further participation in the development process for NIST CSF Version 2.0, and welcomes the opportunity to provide any support needed or answer questions you may have moving forward.

Sincerely,

Jim Guinn
Senior Managing Director
Accenture Security

## General Framework Feedback

*NIST Question: "Usefulness of the NIST Cybersecurity Framework"*

As originally designed, the NIST CSF was created to be a framework for critical infrastructure owners and operators. We understood the CSF to be a starting point for those organizations, particularly those with less experience in developing a cybersecurity program. What we found in the years that followed is that the framework began to be adopted by more than just critical infrastructure companies, and it also became more than just a starting point for many organizations. In many cases companies began to use it as a replacement for the more comprehensive and, as a result, more complicated NIST SP 800-53 or other security control frameworks – including for the largest multi-national organizations.

To be more accessible and approachable, the framework understandably boils down complex ideas and cybersecurity constructs in to simple, short phrases. For example, the category "identity management, authentication and access control" covers an incredibly deep area spanning verifying identity to the concept of the credential itself and how it is managed to how the individual's identity is tied to it and how the system is accessing the credential. These are complex issues and require attention paid to specific controls in NIST SP 800-53 and the other references provided by NIST. Unfortunately these references are often overlooked by organizations.

We applaud NIST for creating a framework that has grown in its usefulness and application to help thousands of companies across the world. We recommend that as NIST develops a CSF update, it takes the opportunity to remind organizations about the purpose of the framework and its usefulness as a starting point, not a complete evaluation of a company's cyber program.

*NIST Question: "Challenges that may prevent organizations from using the CSF or using it more easily or extensively"*

We recommend that NIST consider more clearly identifying how the framework subcategories should be applied in operational technology (OT) environments. The language in the CSF generally favors information technology (IT) systems (ex: identity access management language on securing physical devices, rather than serial devices), and although NIST maps to NIST SP 800-82 by concentration, the CSF does not provide direct references. Providing references to that special publication or even including at some point a separate framework for OT would help organizations use the framework more.

Similarly, the rise in at-home work during the COVID-19 pandemic has brought to light how heavily the framework emphasizes physical security over virtual security. Taking a fresh look at the subcategories considering the changes organizations have faced over the last few years could be beneficial.

We also encourage NIST to consider how to add more context or explanation for the subcategory statements regarding baseline expectations of actions to take to meet each subcategory. Rather than being a "check the box" exercise for organizations, this would help jump-start their internal conversations about what tasks the organization should be performing. The references are a useful tool for deeper conversation. However, in our experience, many organizations fail to use them as intended and, in any case, they are often incomplete. A more explanatory statement for each subcategory that helps organizations understand what a Tier 1, Tier 2, Tier 3, and Tier 4 organization looks like with respect to that subcategory would be useful.

*NIST Question: "Features of the NIST Cybersecurity Framework that should be changed, added or removed"*

Organizations could benefit from more instruction and clarification around the tiering and profile development sections of the CSF. We have found that these tools are rarely used by organizations because they do not understand how or when they should be implemented.

On tiering, although the CSF explains that it is not meant to be a maturity model, the wording used does imply that it indicates maturity and could be modified to provide more clarity.

On the profiles, it is not clear when and how an organization should set a target profile, and in our experience, organizations rarely do so. Providing more detailed instructions on these issues may lead to increased use.

*NIST Question: "Additional ways in which NIST could improve the CSF or make it more useful"*

Finding ways to add more objectivity to the CSF is a challenge, but something we believe NIST should consider in its update. Understanding that we don't want the NIST CSF to become an audit-like process, there could be real benefit to encouraging organizations to collect evidence or other sample data to help validate their self-assessment.

Additionally, we recommend considering cross-referencing the CSF subcategories throughout the framework itself. Many of the subcategories build off other subcategories elsewhere in the framework, and helping an organization understand how they impact and interact with one another would be useful to the organization. For example, the subcategory "the impact of the incident is understood" could be cross referenced back to asset management and criticality ratings.

*NIST Question: "Relationship of the CSF to Other Risk Management Resources"*

Should NIST and the Cybersecurity and Infrastructure Security Agency's (CISA) move forward with its performance goals, developed pursuant to the President's Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, we recommend NIST consider how it can incorporate the goals into the framework.

Initial comments from industry to CISA on its first draft of baseline performance goals focused on questions about what value the initiative offers. When asked in March at Accenture's Operation Next:22 Conference how the performance goals compliment other frameworks and standard initiatives, Executive Assistant Director for Cybersecurity Eric Goldstein described them as helping to answer the question of "how am I doing" as an organization and helping to provide a "set of benchmarks and baselines" and "outcome-based goals." We understand that NIST and CISA will be continuing the refinement process to develop baseline standards, and also plan to develop industry-specific performance goals. NIST should consider whether it would be useful to work to develop performance goals that could be added as references for subcategories, or whether they can be otherwise mapped to the framework in a way that provides maximum value and ensures they can be used effectively by organizations.

*NIST Question: "Cybersecurity Supply Chain Risk Management Guidance"*

NIST requested input on whether and how to integrate Cybersecurity Supply Chain Risk Management Guidance into an updated CSF. In short, we believe that attempting to merge supply chain guidance with the framework would do more harm than good. First, it would elevate supply chain risk management over other risk management issues in a way that could suggest that other issues are less important or detract from their focus. Second, the individuals who are

most likely to use the CSF are generally cyber professionals who may not have control over supply chain risk management and procurement decisions within an organization. Finally, cybersecurity supply chain is even more industry dependent than other aspects of the risk framework. The supply chain section in the CSF already addresses the issue from a baseline perspective. We think that any further guidance should be prepared as part of a separate document.

# RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk

| # | Document | Column *if core spreadsheet* | Line # OR CSF Reference | Comment and Rationale | Recommended Change/Recommended Language |
|---|---|---|---|---|---|
| 1 | Cybersecurity Framework v1.1 | General Framework | | It would useful to provide context for each of the subcategory statements to clarify the expectations for that subcategory. | Add a level to the Framework titled "Expectations" that outlines the general tasks that an organization should perform *at a minimum* to meet the subcategory requirement. |
| 2 | Cybersecurity Framework Core (.xlsx) | Informative References | | The NIST-based mappings into the framework subcategories should be reviewed as they seem to be incomplete and also, in some cases, incorrect. Since there is no context provided except the references, implementers are getting confused and using them as authoritative (complete references that outline the controls that need to be implemented in order to meet the subcategory). | Consider splitting into two reference categories: NIST **authoritative** references (with definitive mappings into NIST 800-53/82) and Non-NIST informative references (mappings into other frameworks and authorities). |
| 3 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.AM-3 | The requirement for mapping "communications and data flows" is not clear. Suggest rewording to require both network and security architectures and data flow diagrams that reflect the current "as operating" state. | Network and security architectures that include data flows between internal and external systems and that reflect the current "as operating" state are developed |
| 4 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.AM-4 | The wording of this requirement is vague and should be reworded for clarity. It also should be moved to the ID.SC category )see note for ID.SC-2). Needs context around what external systems are of interest. The identification of systems external to the organization could be interpreted as anything, although it is assumed the intent is those that belong to service providers or partners with persistent connections into the network, entities providing services such as outsourced security providers, IaaS, Saas, etc.), or other data repositories that hold organizational information. The requirement should be clear on what, exactly, they should be identifying. | External systems and applications that are used to provide services and/or data repositories that hold organizational information are included in hardware and software inventories |
| 5 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.AM-6 | Roles and reponsibilities (R2s) are covered in multiple places throughout the framework (ID.AM-6, ID. BE (Category), ID.GV-2, DE.DP-1, RS.CO-1). Consoidate the requirements for cybersecurity R2s into one subcategory. Consider moving to ID.GV-2. | Cybersecurity roles, responsibilities, accountabilities and authorities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established, communicated, coordinated with, and aligned to internal roles and external partner services |
| 6 | Cybersecurity Framework Core (.xlsx) | Category | ID.BE | Some of the items in this category seems to be a holdover from when the Framework was only targeted toward industrial control systems supporting critical infrastructure (ICS/CI). | Update this section to ensure that implementers understand their business environment regardless of their place in the supply chain or categorization as critical infrastructure; add a requirement that the cybersecurity program is supported by management with visible and tangible backing, personnel, and funding; and require that the organization understand the systems that support the business and their priority to its continued operations (Business Impact Assessment); identify both upstream and downstream dependencies; and plan for resiliency (Businss Continuity Planning/Disaster Recovery). |
| 7 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.BE-(new) | New | The cybersecurity program is supported by organizational management at all levels with visible and tangible backing, personnel, and funding |
| 8 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.BE-1 | This item should be part of the Supply Chain Risk Management plan (ID.SC-1) | Include in ID.SC-1. |
| 9 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.BE-2 | Holdover from Framework v.1 | Remove |
| 10 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.BE-3 | Reword | The critical functions that support the business mission, the systems and applications that support the critical functions, and their priority to its continued operation are identified |
| 11 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.BE-4 | Reword | Upstream and downstream dependencies supporting critical functions, systems, and applications are identified, both external and internal to the organization |
| 12 | Cybersecurity Framework Core (.xlsx) | Category | ID.GV | Governance processes cover more than the subcategories listed, such as the cybersecurity program structure and enforcement and oversight functions. | Added new requirements to consider under GV |
| 13 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.GV-1 | Reword - requiring an organization to have policy is not the same as requiring everyone to use them | Organizational cybersecurity policy and procedures are established, communicated, required for all organizational resources (e.g., hardware, devices, data, personnel, and software), and enforced |
| 14 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.GV-2 | Reword and combine requirements from ID.AM-6 and other subcategories that reference roles and responsibilities | Cybersecurity roles, responsibilities, accountabilities and authorities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established, communicated, coordinated with, and aligned to internal roles and external partner services |

| | B | C | D | E | F | G |
|---|---|---|---|---|---|---|
| 2 | **RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk** | | | | | |
| 3 | **#** | **Document** | **Column** *if core spreadsheet* | **Line # OR CSF Reference** | **Comment and Rationale** | **Recommended Change/Recommended Language** |
| 18 | 15 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.GV-(new) | New | Agreements are in place that outline users' responsibilities for cybersecurity and signifies their understanding of sanctions for non-compliance with cybersecurity policies and procedures |
| 19 | 16 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.GV-(new) | New - while the wording mirrors the category description, there is no requirement for governance processes to be in place | Cybersecurity governance processes are established to provide ongoing management and monitoring of the organization's regulatory, legal, risk, environmental, and operational cybersecurity posture |
| 20 | 17 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.GV-4 | Reword - at this level (GV), organizational governance and risk management processes are usually focused on business risk and safety, and many times cybersecurity is not integrated into business-level processes | Cybersecurity risks are integrated into organizational governance and risk management processes |
| 21 | 18 | Cybersecurity Framework Core (.xlsx) | Category | ID.RA | This section implements ID.RM, and may be better placed under PR | Move to the Protect category |
| 22 | 19 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.RA-(new) or ID.RM-(new) | While this section breaks down the elements of performing a risk assessment, there is no requirement for a risk assessment process to be implemented (note: if ID.RA is moved to PR, place this requirement under ID.RM) | Organizational systems are routinely assessed for risk using established risk assessment processes to confirm they are meeting cybersecurity policy objectives |
| 23 | 20 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID-RM-3 | Reword - holdover from when the Framework was only targeted toward industrial control systems supporting critical infrastructure (ICS/CI); also, tolerance is determined in ID.RM-2 | The organization's determination of cybersecurity risk is informed either by its role in critical infrastructure or using sector-specific threat intelligence |
| 24 | 21 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.RM-(new) | New | Cybersecurity risk management results are communicated to organizational leadership and remediation actions prioritized according to criticality and impact |
| 25 | 22 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.SC-2 | Replace ID.AM-4 with the recommended new verbiage as it seems to be covered here | No change, note only |
| 26 | 23 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-11 | Move PR.IP-11 to PR.AC and change the wording to require that access procedures are integrated with HR. | Access procedures are integrated with Human Resources for account and access initiations, transfers, investigations, and terminations |
| 27 | 24 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-10 | Move to RS.RP-1 (Response) and RC.RP-1 (Recovery) - These belong in the Functions they are associated with. | No change, note only |
| 28 | 25 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-10 | The Business Continuity and Disaster RecoveryPlans | |
| 29 | 26 | Cybersecurity Framework Core (.xlsx) | Subcategory | RS.RP-1 | Move to RS.RP-2 if PR.IP-10 (Response) is moved to RS.RP-1. | New |
| 30 | 27 | Cybersecurity Framework Core (.xlsx) | Subcategory | RC.RP-1 | Move to RS.RP-2 if PR.IP-10 (Recovery) is moved to RC.RP-1. | New |
| 31 | 28 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.AM-1 | "Asset" includes both devices and systems valuable or of importance to the organization. | Physical Assets within the organization are inventoried |
| 32 | 29 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.AM-2 | "Asset" includes software platforms, applications, and systems valuable or of importance to the organization. | Software Assets within the organization are inventoried |
| 33 | 30 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.AM-3 | 1. Add requirement to maintain/update the documentation.<br>2. Remove "communication" as this terms creates confusion. "Communication" in network is communication protocols but "communication" for business purpose is messaging/telecommunication channel. | Organizational data flows are mapped, documented, and maintained |
| 34 | 31 | Cybersecurity Framework Core (.xlsx) | Subcategory | ID.AM-4 | Term consistency for external contractor/service providers | Third-party components and information systems are inventoried |
| 35 | 32 | Cybersecurity Framework Core (.xlsx) | Category | ID.BE | Existing ID.BE category is not valuable as a standalone Category. It is a governance control and should be merged under ID.GV | 1. Merge Business Environment (ID.BE) Category under Governance (ID.GV)<br>2. Merge ID.BE Category requirement as two new Subcategory or merge with existing Subcategories under ID.GV, e.g. (1) The organization's mission, objectives, stakeholders, and activities are identified, documented, and communicated; and (2) The organizations cybersecurity roles, responsibilities, and risk management decisions are identified, documented, and communicated. |
| 36 | 33 | Cybersecurity Framework Core (.xlsx) | Category | ID.RA | Risk assessment process and risks management strategy are inter-dependent | "Risk Assessment (ID.RA)" should be combined with "Risk Management Strategy (ID.RM)" as "Risk Management" Category |
| 37 | 34 | Cybersecurity Framework Core (.xlsx) | Category | ID.SC | N/A | The guidance in ID.SC Subcategories is more detailed compared to the rest of the older Subcategories. In general, all Subcategories should have this same level of guidance. |
| 38 | 35 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.AC-1 | "Asset" includes devices, systems, software, etc. valuable or of importance to the organization. | Identities and credentials are issued, managed, verified, revoked, and audited for authorized assets, users and processes |
| 39 | 36 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.AC-3 | Increased use of portable devices | Add requirement for remote wipe enforcement for portable physical assets |
| 40 | 37 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.AC-6 | Confusing wording | Update guidance to use relevant authentication and authorization terminology |

| | B | C | D | E | F | G |
|---|---|---|---|---|---|---|
| 2 | **RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk** | | | | | |
| 3 | **#** | **Document** | **Column** *if core spreadsheet* | **Line # OR CSF Reference** | **Comment and Rationale** | **Recommended Change/Recommended Language** |
| 41 | 38 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.AT-4 | "Management" includes executive, leadership, and managerial roles | Cybersecurity management understand their roles and responsibilities |
| 42 | 39 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.DS-1 | Add PR.DS-5 requirements here. | "Data-at-rest is protected and data leakage prevention is implemented" |
| 43 | 40 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.DS-2 | Add PR.DS-5 requirements here. | "Data-in-transit is protected and data leakage prevention is implemented" |
| 44 | 41 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.DS-3 | "Securely" is more appropriate for the intention, instead of "formally". | Add more guidance to this high-level recommendation<br>"Assets are securely managed throughout removal and transfers according to the organization's data management processes" |
| 45 | 42 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.DS-5 | Merged with PR.DS-1 and PR.DS-2 | Deleted - merged |
| 46 | 43 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.DS-6 | Switch ordering with "PR.DS-7". Suggested order of Subcategories are as follows: | PR.DS-6: The development and testing environment(s) are separate from the production environment<br>PR.DS-7: Integrity checking mechanisms are used to verify software, firmware, and information integrity<br>PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity |
| 47 | 44 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-1 | Existing guidance is very high-level. Separate into three Subcategories according to Physical Asset, Information Systems and Software Assets.<br>2. Include PR.IP-2 to the base configuration guidance for software assets. | |
| 48 | 45 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-2 | Existing guidance is very high-level. Separate into three Subcategories according to Physical Asset, Information Systems and Software Assets.<br>2. Include PR.IP-2 to the base configuration guidance for software assets. | |
| 49 | 46 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-5 | Wide use of virtual environment | Include virtual environment. "Policy and regulations regarding the physical and **virtual** operating environment for organizational assets are met" |
| 50 | 47 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-6 | Sentence structure consistency | Reword: "Data disposal processes are in place and managed" |
| 51 | 48 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-7 | Combine PR.IP-7 and PR.IP-8, to say | "Protection processes are in place and managed, and effectiveness of protection technologies are measured" |
| 52 | 49 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-8 | Combine PR.IP-7 and PR.IP-8, to say | "Protection processes are in place and managed, and effectiveness of protection technologies are measured" |
| 53 | 50 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-9 | Combine PR.IP-9 and PR.IP-10, to say | "Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place, managed, and tested" |
| 54 | 51 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.IP-10 | Combine PR.IP-9 and PR.IP-10, to say | "Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place, managed, and tested" |
| 55 | 52 | Cybersecurity Framework Core (.xlsx) | Subcategory | PR.PT-4 | Reword it to say: "Network architecture, configuration process, and network management are protected" | Reword it to say: "Network architecture, configuration process, and network management are protected" |
| 56 | 53 | Cybersecurity Framework Core (.xlsx) | Subcategory | DE.AE-1 | DE.AE-1 and DE.AE-5 are baseline config requirements. Move DE.AE-5 after "DE.AE-1". Reorder the sub-categories to be: | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed<br>DE.AE-2: Incident alert thresholds are established<br>DE.AE-3: Detected events are analyzed to understand attack targets and methods<br>DE.AE-4: Event data are collected and correlated from multiple sources and sensors<br>DE.AE-5: Impact of events is determined |
| 57 | 54 | Cybersecurity Framework Core (.xlsx) | Subcategory | DE.AE-5 | DE.AE-1 and DE.AE-5 are baseline config requirements. Move after "DE.AE-1". Reorder the sub-categories to be: | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed<br>DE.AE-2: Incident alert thresholds are established<br>DE.AE-3: Detected events are analyzed to understand attack targets and methods<br>DE.AE-4: Event data are collected and correlated from multiple sources and sensors<br>DE.AE-5: Impact of events is determined |
| 58 | 55 | Cybersecurity Framework Core (.xlsx) | Subcategory | DE.CM-2 | Wide use of virtual environment | Physical and virtual environment are monitored to detect potential cybersecurity events |
| 59 | 56 | Cybersecurity Framework Core (.xlsx) | Subcategory | DE.CM-6 | Term consistency for external contractor/service providers | Third-party service provider activity is monitored to detect potential cybersecurity events |

| | B | C | D | E | F | G |
|---|---|---|---|---|---|---|
| 2 | **RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk** | | | | | |
| 3 | **#** | **Document** | **Column** *if core spreadsheet* | **Line # OR CSF Reference** | **Comment and Rationale** | **Recommended Change/Recommended Language** |
| 60 | 57 | Cybersecurity Framework Core (.xlsx) | Subcategory | RS.RP-1 | Reword | Response plan is in place ready to be executed during an incident; managed, and tested periodically and after an incident |
| 61 | 58 | Cybersecurity Framework v1.1 | General Framework | | Due to increase in remote workforce and virtual environment, controls that currently focus on physical security should be extended to include virtual security | |
| 62 | 59 | Cybersecurity Framework v1.1 | General Framework | | In general, NIST CSF Subcategories should be expanded to provide additional guidance and minimize "organizational interpretation" approach. Subcategories in ID.SC are the latest controls added in V1.1 and they have adequate detailed guidance | |
| 63 | 60 | Cybersecurity Framework v1.1 | General Framework | | Rename Subcategories to Controls or Safeguards to align with the naming convention in NIST 800-53 and other industry standards | |
| 64 | 61 | Cybersecurity Framework v1.1 | General Framework | | Make Subcategory numbering more numerical, e.g. ID.AM-1 can be ID.01.01. Current format causes a lot of confusion during review, e.g. RS.MI vs. RS.IM vs. RC.MI, and PR.AT vs. PR.AC vs. PR.PT, etc. | |
| 65 | 62 | Cybersecurity Framework v1.1 | General Framework | | In Framework worksheet separate existing Subcategory numbering to another column for easy filtering and re-ordering. I.e., Functions – Category – Subcategory – Subcategory Details | |
| 66 | 63 | Cybersecurity Framework v1.1 | General Framework | | In Framework worksheet move Information Reference to another tab within the worksheet. The merged cells in Subcategory make it difficult to filter the Subcategories | |
| 67 | 64 | Cybersecurity Framework Core (.xlsx) | Subcategory | DE.AE-1 | Users should include detection into their network/cyber architecture planning. | Event detection is incorporated into the enterprise cybersecurity architecture plan |
| 68 | 65 | Cybersecurity Framework Core (.xlsx) | Subcategory | DE.CM-5 | remove 'mobile' and have this point to all devices. No reason to point out mobile specifically, it limits the conversation. | Unauthorized code is detected |
| 69 | 66 | Cybersecurity Framework Core (.xlsx) | Subcategory | DE.CM-8 | This fits better in identify. And is a double from ID.RA-1 | remove and add language to ID.RA-1 about continuous scans being performed. |
| 70 | 67 | Cybersecurity Framework Core (.xlsx) | Category | DE.DP | This section should include a subcategory for response playbooks | Playbooks are generated and followed for applicable detected events. Playbooks are continuously improved. |
| 71 | 68 | Cybersecurity Framework Core (.xlsx) | Function | RC | Many during the assessments confuse incident recovery with disaster recovery and business continuity, when they are two different things that sometimes work together.<br><br>In PR.IP-9 there is a separation between Incident Recovery and Deisaster Recovery, but not in RC section.<br><br>Containment and Mitigation should be focus of recovery, and should be made clear the difference between cyber incident recovery and business continuity/disaster recovery. RS.MI might belong in recovery. | Add a subcategroy in<br>RC.RP: Cyber Incident Recovery is incorporated into the Cyber Incident Reponse plan.<br>RC.RP: Personnel know their roles and order of operations when recovery is needed.<br>RC.RP: Cyber Incident Recovery plans include Business Continuity/Disaster Recovery processes and personnel, when establish criteria are met and where applicable. |
| 72 | 69 | Cybersecurity Framework Core (.xlsx) | Function | PR & RS & RC | PR.IP-10 and PR.IP-9 Should move to RS or RC | Language about testing the Incident Response plan should be in the Response or Recover sections. |
| 73 | 70 | Cybersecurity Framework Core (.xlsx) | Function | ALL | There should be more cross referencing between the subcategories.<br><br>Ex. Detection has DE.AE-4: Impact of events is determined. There should be a reference to ID with asset management and asset criticality ratings. | |
| 74 | 71 | Cybersecurity Framework Core (.xlsx) | Function | ALL | Guidance should be given on how to leverage the CSF within an ICS/OT environment. | Optimal would be an ICS/OT CSF and an IT CSF which can be leveraged for the separate environments. Most areas would be the same, but language to the specific environments should be included. C2M2 does this with an Electrical Subsector version and an Oil and Gas version. |
| 75 | 72 | Cybersecurity Framework Core (.xlsx) | Function | ALL | More about cybersecurity architecture should be in the frameowk. Strategies around network security, data security, endpoint security, and software security should be incorporated into an overall security architecture strategy. | Incorporate Architecture as a category within Protect with subcategory each for network, data, asset, and software security. |
| 76 | 73 | Cybersecurity Framework Core (.xlsx) | Function | ALL | Funding and resources should be a discussion topic in ID.BE | Add subcategory:<br>ID.BE-X: Cybersecurity funding and current resources is adequate for maintenance of cybersecurity objectives and goals. |

| | B | C | D | E | F | G |
|---|---|---|---|---|---|---|
| 2 | **RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk** | | | | | |
| 3 | **#** | **Document** | **Column** *if core spreadsheet* | **Line # OR CSF Reference** | **Comment and Rationale** | **Recommended Change/Recommended Language** |
| 77 | 74 | Cybersecurity Framework Core (.xlsx) | Function | ID | Vulnerability identification and management should be it its own subcategory. | |
| 78 | 75 | Cybersecurity Framework Core (.xlsx) | Category | DE.CM | DE.CM should be first in Detect function. | |
| 79 | 76 | Cybersecurity Framework Core (.xlsx) | Category | DE.DP | There should be language around delineation/distinction between a Cyber Event and a Cyber Incident, with reference to Response subcategory which identifies incident response plans. | |
| 80 | 77 | Cybersecurity Framework Core (.xlsx) | Category | DE.CM | Client Off-prem monitoring approaches should be identified specifically as a subcategory | |