Comment Matrix - NIST Doc

Comment Number	Date	Commenter Name	Comment	Location of Change (Page number, Section, Header, Paragraph, Line #)
1	5/7/2023	Stephanie Saravia	GV.OC-02 and GV.OC-03 appear to be very similar Subcategories. It seems like the "external stakeholders" in GV.OC-02 would be covered by GV.OC-03. The only unique aspect of GV.OC-02 seems like internal stakeholders. Recommend modifying the words to make a clear distinction, or adding examples to clarify the difference.	pg 6, Table 3, CSF 2.0 Subcategories GV.OC-02 & -03
2	5/7/2023	Stephanie Saravia	GV.OC-02 and GV.OC-03 appear to be very similar Subcategories. It seems like the "external stakeholders" in GV.OC-02 would be covered by GV.OC-03. The only unique aspect of GV.OC-02 seems like internal stakeholders. Recommend modifying the words to make a clear distinction, or adding examples to clarify the difference.	pg 6, Table 3, CSF 2.0 Subcategories GV.OC-02 & -03
3	5/7/2023	Stephanie Saravia	GV.OC-04 and GV.OC-05 appear to be very similar Subcategories. Recommend modifying the words to make a clear distinction, or adding examples to clarify the difference.	pg 6-7, Table 3, CSF 2.0 Subcategories GV.OC-04 & -05
4	5/7/2023	Stephanie Saravia	GV.RM-04: recommend to change the word "enterprise." This reads as though the OT risk management process for cybersecurity should get absorbed by the Enterprise risk management process. I believe the intent is for all cybersecurity risk management processes to be aligned with & incorporated into the corporate risk management strategy. This may need to be "organization" instead of "corporate" for consistency; however, "organization" makes it sound like you can self-contain a cyber risk assessment within the cyber organization. Cybersecurity risk management is considered part of the corporate risk management strategy.	pg 7, Table 3, CSF 2.0 Subcategory GV.RM-04
5	5/7/2023	Stephanie Saravia	GV.RR-02, -03, and -04 appear to be very similar. Recommend modifying the words to make a clear distinction, or adding examples to clarify the difference. Recommend -02 include the word internal, or organizational members. We have written: customers, partners, other third-party stakeholders, and suppliers. How would that list translate to examples? Why would suppliers have contractual language, but customers don't? What I have in mind for examples: partner = joint venture companies; suppliers = upstream companies, component suppliers (Dell, Rockwell, GE, etc.), Internet Service Providers, power, water, natural gas; third-party stakeholder = ? perhaps contractors that have remote access to computing equipment, contractors with physical access to equipment, external auditors & assessors; customers = downstream companies Very often, customers will have network connections to the organization which would require contractual language the same as what is required for a supplier. How would you handle Incident Response R&R? Where to government entities and first responders fall into the R&R? Each company should have some relationship with their SRMA. Where/how should an organization document the organization:SRMA R&Rs?	pg 8, Table 3, CSF 2.0 Subcategories GV.RR-02, -03, -04
6	5/4/2023	jason crossland	GV.RR-05: Lines of communication across the organization are established for cybersecurity risks, including supply chain risks; there are all kinds of "cybersecurity risks focused areas" Along with SCRM, the top 3 should be listed. Also, should say "are established and managed for cybersecurity risks, including...."	pg 9, Table 3, CSF 2.0 Function-Section- "GV.RR"
7	5/7/2023	Stephanie Saravia	GV.PO-02: Recommend to reword or remove. This does not seem enforceable as-stated. For example, a large manufacturing corporation will have a structured set of policies regarding cybersecurity. Manufacturing facilities require specialty parts based on their chemical composition, unique process, etc. They will leverage small companies as suppliers for these unique components. A 10-person component supplier cannot possibly apply the same policies as a 100,000-person manufacturing organization. Since this is not enforceable, recommend to delete. I believe the intent of GV.PO-02 is captured within GV.RR-04.	pg 9, Table 3, CSF 2.0 Subcategory GV.PO-02
8	5/4/2023	jason crossland	GV.PO-03: Policies and procedures are reviewed, updated, and communicated to reflect changes in requirements, threats, technology, and organizational mission. Should also include; "vulnerabilities, risk posture and resources"	pg 9, Table 3, CSF 2.0 Function-Section- "GV.PO"
9	5/4/2023	jason crossland	ID.AM-03: Representations of the organization's authorized network communication and network data flows are maintained (formerly ID.AM-3 and DE.AE□1). Should also include "Ports, Protocols, & Services (PPS's), and network data flows..."	pg 9, Table 3, CSF 2.0 Function-Section- "ID.AM"
10	5/7/2023	Stephanie Saravia	ID.AM-04: Recommend Inventories of external network-connected assets are maintained. Rationale: There are no bounds to the term "external assets." I believe we are targeting those external systems which could present a cyber risk to our network. Similarly, the term suppliers has no bounds. We don't need a list of every supplier of bolts, screws, etc. for cybersecurity purposes. I believe what we want is a listing of make, model, version #, and distributor for our computing assets. This listing of asset details, including supplier information, should be included in the asset inventory and associated with the asset.	pg 10, Table 3, CSF 2.0 Subcategory ID.AM-04
11	5/4/2023	jason crossland	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and organizational value. Would add "mission dependency mapping/linkages"	pg 10, Table 3, CSF 2.0 Function-Section- "ID.AM"

12	5/4/2023	jason crossland	ID.AM-08: Systems, devices, and software are managed throughout their life cycle, including pre-deployment checks, preventive maintenance, transfers, end-of-life, and disposition (formerly PR.DS-3, PR.IP-2, PR.MA-1, and PR.MA-2). SDLC also includes prequirement/acquistion; Would add "procurement/acquisition, sustainment...."	pg 10, Table 3, CSF 2.0 Function-Section- "ID.AM"
13	5/7/2023	Stephanie Saravia	ID.RA-01: Recommend Asset vulnerabilitites are identified, validated, and recorded. Rationale: There are no bounds to "third-party assets," making this Subcategory impossible to achieve. A third-party company has no requirement to disclose their architecture or asset details - and they shouldn't, for their own cyber protection.	pg 11, Table 3, CSF 2.0 Subcategory ID.RA-01
14	5/4/2023	jason crossland	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources. Would add "Cyber threat intelligence is received and analyzed for operational applicability from....."	pg 11, Table 3, CSF 2.0 Function-Section- "ID.RA"
15	5/7/2023	Stephanie Saravia	ID.RA-10: This Subcategory addresses **exceptions** to "security measures," but no where in the CSF do we tell people to **apply** "security measures." Recommend to either incorporate "security measures" into a different ID.RA, or change the language in ID.RA-10 to be consistent with ID.RA-06. (Preferred) ID.RA-06: **Security measures** are chosen, prioritized, planned, tracked, and communicated. OR ID.RA-10: Exceptions to **risk responses** are reviewed, tracked, and compensated for.	pg 12, Table 3, CSF 2.0 Subcategory ID.RA-10
16	5/7/2023	Stephanie Saravia	Recommend to review how external organizations are referred, and ensure they are intentionally included/excluded from Subcategories. Observed below are differences in how organizations are labeled & included within the CSF 2.0. GV.RR-03: customers, partners, and other third-party stakeholders GV.RR-04: suppliers ID.SC-03: suppliers and third-party partners ID.IM-02: suppliers and third-party partners PR.AT-03: suppliers, partners, customers What's the difference between partner, third-party stakeholder, and third-party partner? Should customers be included in ID.SC-03 and ID.IM-02?	Table 3, throughout
17	5/7/2023	Stephanie Saravia	PR.IR-01: Recommend to relocate to Response and Recovery functions. It doesn't seem to fit as a Protection function. Recommend this to be broken into 4 Subcategories: RS.MA-X: An incident response plan is developed, approved, and maintained. RS.MA-Y: An incident response plan is communicated and tested. RC.RP-A: A recovery plan is developed, approved, and maintained. RC.RP-B: A recovery plan is communicated and tested. Rationale: 1) CSF includes communication and execution of the plans, yet their development is not addressed. 2) ID.IM-02 says "security tests and exercises..." The term "security tests" sounds like a validation of security controls such as verification of detection and protection tools. I feel like response and recovery plan testing should be explicitly mentioned as a separate Subcategory. 3) Recommending to remove the "(e.g., IRP, BCP, DRP, and CP)" reference in PR.IR-01. These plans are overlapping and confusing. NIST SP 800-34 acknowledges this confusion. "In general, universally accepted definitions for information system contingency planning and the related planning areas have not been available... Because of the lack of standard definitions for these types of plans, the scope of actual plans developed by organizations may vary from the descriptions below." This update to the CSF is an opportunity to simplify NIST's reference to the many plans. I'd recommend "incident response plan" and "recovery plan" for cybersecurity purposes.	pg 20, Table 3, CSF 2.0 Subcategory PR.IR-01
18	5/4/2023	jason crossland	PR.IR-02: The organization's networks and environments are protected from unauthorized logical access and usage (formerly PR.AC-3, PR.AC-5, PR.DS-7, and PR.PT-4). Would add "…are protected from unauthorized logical and physical access and usage."	pg 20, Table 3, CSF 2.0 Function-Section- "PR.IR"
19	5/4/2023	jason crossland	PR.PS-05: Protective technologies are executed on or within platforms to stop unauthorized software execution. "Protective" technologies can be broken down into different areas; Computing Environments, Boundary, and High Assurance Protections. High Assurance- can be considered Data Protection (e.g., software). Would add language that speaks to Computing (network) & Boundary (PPS's) under PR.PS Category.	pg 20, Table 3, CSF 2.0 Function-Section- "PR.PS"
20	5/7/2023	Stephanie Saravia	Recommend reordering DE.CM above DE.AE. Each of the CM subcategories includes "to find adverse cybersecurity events." The AE subcategories address what to do once you've found the event. My preference is to have CM above AE for chronological ordering.	pg 21-22, Table 3, CSF 2.0 Categories AE and CM
21	5/17/2023	Carlton Gray	How does the CSF 2.0 work for smaller organizations, or business with out a large IT, OT staff?	
22	5/17/2023	Carlton Gray	Will the CSF 2.0 be digitized with access to vulnerability information?	
23	5/17/2023	Carlton Gray	How will CSF 2.0 work with AI to reduce vulnerabilities and strengthen defenses?	
24	5/17/2023	Carlton Gray	Does the CSF 2.0 assist with assigning roles and responsibilities within the organization?	
25	5/17/2023	Carlton Gray	Does the CSF 2.0 prioritize organizational mission objectives?	
26	5/17/2023	Carlton Gray	Does the CSF 2.0 incorporate or suggest the best fit NIST policies or procedures to assist an organization to make a decision.	

27	5/17/2023	Carlton Gray	Does the CSF 2.0 require the DoD to implement new policies or procedures to implement?	
28	5/17/2023	Carlton Gray	Does the CSF 2.0 increase the workload for those using the RMF process and if so specifically how?	
29	5/17/2023	Carlton Gray	How will the CSF 2.0 assist organizations to identify supply chain management issues?	
30	5/17/2023	Carlton Gray	How will the CSF 2.0 assist with addressing industrial control systems ?	
31	5/17/2023	Carlton Gray	If the CSF 2.0 is used in conjunction with other frameworks why not just improve an existing framework?	
32	5/17/2023	Carlton Gray	Will the CSF 2.0 create a universal measurement and assessment process that can be applied across all organizations.	
33	5/17/2023	Carlton Gray	As the CSF 2.0 grows will there be user training available for organizations?	
34	5/17/2023	Carlton Gray	As Tier levels increase in rigor and sophistication what training will be offered?	
35	5/17/2023	Carlton Gray	Will the various tier levels assist organizations I obtaining an ATO?	
36	5/17/2023	Carlton Gray	Will the CSF 2.0 take into considerations organizational certifications such as the CMMC	