Comments template for Preliminary
Cybersecurity Framework

Submitted by: Tacoma Public Utilities
Date: 12/13/2013

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	ii & 13	40	TOC	The Framework Core is the core of the Framework, and should therefore not be an appendix to the Framework.	Move the Framework Core to it's own section within the main body of the document.
2	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	9	321-389	Framework Implementation Tiers	There is no tier available for organizations that truly have NO program in place or have no achievement in a specific Function/Category/Subcategory, and therefore they cannot assess their current maturity accurately. Not having a Tier 0 as a starting point is like having a speedometer that starts at 10 mph, with no way to measure if you have come to a complete stop.	A Tier 0 is necessary to complete the Implementation Tiers. Defined as: Tier 1 has not been achieved.
3	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	11	392	How to Use the Framework	In order for the framework to be able to be used to establish a NEW cybersecurity program as indicated by this line, a Tier 0 must be available.	A Tier 0 in the Implementation Tiers section is necessary in order to allow this framework to aid in establishing a new cybersecurity program.
4	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	12	425-431	Step 5: Determine, Analyze, and Prioritize Gaps.	The Framework must provide a context to allow prioritization without requiring additional resources be added or implemented. This is required by the EO.	Add a prioritization example, with resources to determine risk referencing high probability vulnerabilities, etc.
5	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	13	457-467	Appendix A: Framework Core	Same comment as #1, the Framework Core is the Framework, and should be expressed in the body of the document, not as an appendix (defined as a section or table of additional matter at the end of a book or document.)	Move the Framework Core into the body of the document.
6	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	17		PR.AC-5: Network integrity is protected	Network Integrity may be an outcome of much more than just Network Access Control.	

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
7	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	20		PR.IP-6: Information is destroyed according to policy and requirements	according to a documented policy	according to a documented policy
8	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	20		PR.IP-7: Protection processes are continuously improved	Why is this a Subcategory and not expressed in a Tier? Applying this to only two subcategories within the Framework gives the impression that it is not necessary elsewhere.	Remove and express continuous improvement as a Tier.
9	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.PT-1: Audit and log records are stored in accordance with audit policy	accordance with a documented audit policy	accordance with a documented audit policy
10	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	23		DE.DP-5: Detection processes are continuously improved	Why is this a Subcategory and not expressed in a Tier? Applying this to two subcategories gives the impression that it is not necessary elsewhere.	Remove and express continuous improvement as a Tier.
11	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	24		RS.CO-2: Events are reported consistent with established criteria	regulatory requirements should be added here	add "and regulatory requirements" to the end of this subcategory.
12	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RS.AN-4: Incidents are classified consistent with response plans	consistent with documented response plans	consistent with documented response plans

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
13	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	13	464	Appendix A: Framework Core	add definition within this selection process.	Change the last sentence to read "An organization’s risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection and definition of these activities during Profile creation."
14	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	28		Appendix B: Methodology to Protect Privacy and Civil Liberties	Privacy section should be applied at a higher level for data privacy relative to Critical Infrastructure Functions	Modify the language in Privacy section away from PII to data privacy in general terms, with examples for sector specific issues, such as energy, financial, technology etc. Allow the audience to understand that the critical information that must remain private varies by sector, i.e. critical infrastructure information vs. PII vs. software codebase, etc.
15	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	28		Appendix B: Methodology to Protect Privacy and Civil Liberties	TWPR supports the Alternative Appendix B being circulated in the Hogan Lovells Comments of December 5, 2013.	Adopt the Alternative Appendix B in its entirety.
16	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	13-25		Appendix A: Framework Core	Include NERC CIP Standards as informative References throughout the Framework Core	Add the NERC CIP Standards Mapping developed by DOE and NERC to each category and subcategory. http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United States

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
17	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	7-8	281-306	2.0 Framework Basics	This new text replaces the original text starting from line 281 and ending at line 306.	2.2 Framework Profile A Framework Profile ("Profile") is a tool to enable organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organization and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. A Framework Profile can be used to describe both the current state and the desired target state of specific cybersecurity activities, thus revealing gaps that can be addressed to meet cybersecurity risk management objectives. Figure 2 shows the two types of Profiles: Current and Target. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. The Target Profile is built to support critical infrastructure requirements and aid in the communication of risk within and between organizations. The Profile is the alignment of the Functions, Categories, Subcategories and industry standards with the business requirements, risk tolerance, and resources of the organization. The prioritization of the gaps is driven by the selection of the Framework Tier and organization's Risk Management Processes which can serve as an essential part for resource and time estimates needed that are critical to prioritization decisions .
18	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	9	332	2.4 Framework Implementation Tiers	This is alternative text for the Tier 0 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 0: Not Initiated o Tier 1 has not been achieved.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
19	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	9	332-346	2.4 Framework Implementation Tiers	This is alternative text for the Tier 1 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 1: Initiated o Framework Functions – The implementation of the Framework Functions are not formalized and may be ad hoc, irregular, and sometimes reactive to cybersecurity events. o Risk Management Process – The critical infrastructure cybersecurity risk management practices are not formalized and risk is managed in an ad hoc, irregular and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or critical infrastructure business/mission requirements. o Integrated Program – There is a limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or inadequate resources. o Information Sharing – The organization may not have processes that enable cybersecurity information to be shared within the organization. An organization may not have the processes in place to participate in coordination or collaboration with other entities.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
20	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	10	347-357	2.4 Framework Implementation Tiers	This is alternative text for the Tier 2 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 2: Risk-Informed o Framework Functions – The implementation of the Framework Functions are approved by management, include limited information about cybersecurity risks, but may not be documented in policy. o Risk Management Process – The critical infrastructure risk management practices are approved by management but may not be established as documented policy. o Integrated Program – There is an awareness of cybersecurity risk at the critical infrastructure operations level but an integrated, overall organization-wide approach to managing critical infrastructure cybersecurity risk has not been established. Risk-informed processes and procedures are identified. Cybersecurity personnel resources have been identified but may not be dedicated to or have sufficient knowledge and skills to perform their cybersecurity duties. o Information Sharing – Cybersecurity information is shared within the organization on an informal basis. The organization knows its role in the larger critical infrastructure ecosystem, but has not formalized its capabilities to interact and share information externally.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
21	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	10	358-370	2.4 Framework Implementation Tiers	This is alternative text for the Tier3 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 3: Repeatable o Framework Functions – The implementation of the Framework Functions are formally approved by management expressed in policy and receive adequate resources for sustainability. o Risk Management Process – The critical infrastructure risk management practices are formally approved by management and expressed as policy. The cybersecurity practices are regularly updated based on the application of risk management processes to a changing threat and technology landscape. o Integrated Program – There is a formalized approach to manage cybersecurity risk for the critical infrastructure operations. Repeatable, risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. Consistent methods are in place to effectively respond to changes in risk. There are adequate personnel resource who possess the knowledge and skills to perform their appointed cybersecurity roles and responsibilities. o Information Sharing – Cybersecurity information is shared in a consistent documents process within the organization. The organization understands its dependencies and partners and receives information from these

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
22	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	10	371-385	2.4 Framework Implementation Tiers	This is alternative text for the Tier 4 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 4: Adaptive o Framework Functions – The implementation of the Framework Functions are continuously monitored to ensure they are still meeting the intended cybersecurity risk management outcomes. o Risk Management Process – The critical infrastructure risk management practices are implemented in a manner that allows the organization to readily adapt its cybersecurity practices based on lessons learned and predictive indicators derived from previous cybersecurity activities. Through a process of continuous improvement, the organization actively adapts to a changing cybersecurity landscape and responds to emerging/evolving threats in a timely manner. o Integrated Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks. o Information Sharing – The organization

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
23	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	11	402-436	3.2 Using the Framework	Reworded the steps to create a close connection between the identification of Current Profile, the use of the Framework Core, a Target Profile and a continuous improvement cycle.	3.2 Using the Framework The following recursive steps illustrate how an organization could use the Framework Core, Profiles and Tiers to assess and update an existing cybersecurity program; or create a new cybersecurity program. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to create an action plan for targeted improvements. Step 1: The organization identifies the scope of the critical infrastructure operations that will be assessed in the Step 2 activity. The organization identifies relative to their critical infrastructure operations, systems and assets, the associated risk tolerances, threats, vulnerabilities, constraints, impacts of a cybersecurity event, voluntary and mandatory regulatory requirements and overall risk management approach. The organization also selects the appropriate Framework Informative References or chooses other Informative References that are sector or organization specific. Step 2: The organization develops a Current Framework Profile using each of the Framework Core Functions, Categories and Subcategories. The organization performs an assessment of their existing critical infrastructure cybersecurity
24	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	13-26		Framework Core	Make it clear that the Framework applies to Critical Infrastructure Functions, not all business systems This is further defined in subsequent comments.	Insert "critical Infrastructure" references as appropriate throughout the subcategory descriptions

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
25	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	13		Asset Management (AM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure personnel, devices, systems, facilities and information are identified and managed consistent with their relative importance to risk management practices.
26	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T				Systems, software, hardware, data flows, etc are all identified, but there is no data classification in this Function.	Add a subcategory: For critical infrastructure, the data and information is classified and labeled
27	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	13		ID.AM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical assets and systems are inventoried
28	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	13		ID.AM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the software platforms and applications are inventoried
29	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	13		ID.AM-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the communication data flows are mapped
30	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	14		ID.AM-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the internal and external system interfaces are identified documented and mapped
31	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	14		ID.AM-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the personnel resources are prioritized …

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
32	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	14		ID.AM-6	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the personnel roles and responsibilities for cybersecurity in IT and ICS are identified, documented, communicated and managed
33	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	14		Business Environment (BE)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the mission, objectives….
34	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	14		ID.BE-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the supply chain cybersecurity requirements are identified and communicated
35	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	14		ID.BE-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the role in their industry ecosystem is identified, documented and communicated
36	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	14		ID.BE-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the mission and business objectives and activities are identified, documented, prioritized and communicated
37	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	14		ID.BE-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the internal and external dependencies are identified, documented and communicated
38	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		ID.BE-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the resiliency requirements are identified, documented, prioritized and communicated

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
39	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		Governance (GV)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the policies, procedures and processes to manage and monitor the regulatory, legal, risk, environmental and operational requirements are understood and inform the management of cybersecurity risk.
40	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		ID.GV-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity policy(ies) are identified, documented and communicated
41	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		ID.GV-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity roles and responsibilities are established and communicated
42	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		ID.GV-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the legal and regulatory requirements for cybersecurity, including privacy and civil liberties obligations, are identified, documented and communicated
43	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		ID.GV-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the governance model includes cybersecurity practices
44	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		Risk Assessment (RA)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity risk to operations, including mission and business, image and reputation, assets and individuals is documented
45	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		ID.RA-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the asset vulnerabilities are identified, documented and prioritized for risk response and integrated into the cybersecurity program

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
46	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	15		ID.RA-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the threat and vulnerability information is received from information sharing forums and sources and integrated into the cybersecurity program
47	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		ID.RA-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the threats to assets are identified, documented, prioritized for risk response and integrated into the cybersecurity program
48	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		ID.RA-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the threat and vulnerability impacts are identified, documented, prioritized for risk response and integrated into the cybersecurity program
49	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		ID.RA-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity threat and vulnerability risk responses are identified, documented, prioritized for risk response and integrated into the cybersecurity program
50	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		Risk Management Strategy (RM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure cybersecurity risk management strategy is established and includes priorities, constraints, risk tolerances, and assumptions to support cybersecurity risk decisions
51	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		ID.RM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity risk management processes are identified, documented, prioritized for risk response, and integrated into the cybersecurity program
52	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		ID.RM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity risk tolerances are identified, documented, prioritized for risk response, and integrated into the cybersecurity program.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
53	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		ID.RM-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the determination of risk tolerance is informed by the role in their industry and any sector specific risk analysis
54	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		Access Control (AC)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure accesses to associated information resources and facilities are limited to authorized people processes, systems, and activities.
55	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	16		PR.AC-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the identities and credentials for systems and people is identified, documented and managed.
56	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	17		PR.AC-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical access is identified, documented and managed.
57	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	17		PR.AC-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the remote access to systems is identified, documented, and managed.
58	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	17		PR-AC-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the access permissions to systems is identified, documented, and managed
59	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	17		PR-AC-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the processes for maintaining network integrity is identified, documented, and managed

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
60	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	17		Awareness and Training (AT)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure personnel and partners are adequately trained to perform their cybersecurity related duties and responsibilities consistent with established policies, procedures and agreements.
61	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	17		PR.AT-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the people accessing facilities and systems are informed and trained on their cybersecurity responsibilities
62	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	17		PR.AT-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the privileged users are informed and trained on their cybersecurity responsibilities
63	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	18		PR.AT-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the third-party stakeholders, including customers and partners are informed and trained on their cybersecurity responsibilities
64	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	18		PR.AT-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the senior executives are informed and trained on their cyber security responsibilities
65	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	18		PR.AT-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical security and cybersecurity personnel are informed and trained on their cybersecurity responsibilities
66	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	18		Data Security (DS)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure records and data are managed consistent with the organization's risk management strategy to protect the confidentiality, integrity and availability.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
67	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	18		PR.DS-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the data at rest is protected based on the risk management strategy
68	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	18		PR.DS-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the data in motion is protected based on the risk management strategy
69	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	18		PR.DS-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the assets are managed throughout their entire lifecycle of acquisition, implementation, redeployment and destruction is protected based on the risk management strategy
70	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		PR.DS-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the availability requirements are identified, documented and managed based on the risk management strategy
71	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		PR.DS-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the protections against data leakage of confidential information are identified, documented and managed based on the risk management strategy
72	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		PR.DS-6	Covered in PR.DS-5	Remove this requirement.
73	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		PR.DS-7	Covered in PR.DS-3	Remove this requirement.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
74	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		PR.DS-8	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the development and testing environments are separated from production based on the risk management strategy
75	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		PR.PDS-9	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the privacy of individuals and personally identifiable information (PII) is protected based on the risk management strategy
76	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		Information Protection Processes and Procedures (IP)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure cybersecurity policy addresses the purpose, scope, roles, responsibilities, management commitment and coordination; processes and procedures are maintained and used to manage the protection of critical infrastructure systems.
77	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		PR.IP-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the configuration management baseline is identified, documented and managed
78	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	19		PR.IP-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Systems Development Lifecycle is identified, documented and managed
79	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	20		PR.IP-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the configuration management and change control processes are identified, documented and managed
80	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	20		PR-IP-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the system backups are identified, documented and managed

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
81	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	20		PR.IP-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	what does this one mean?
82	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	20		PR.IP-6	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the confidential information is destroyed according to documented policies and procedures
83	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	20		PR.IP-7	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the policies and procedures that support the Information Protection Processes and Procedures are continuously approved according to the cybersecurity risk management strategy
84	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	20		PR.IP-8	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the sharing of relevant threat and vulnerability information occurs with appropriate parties
85	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	20		PR.IP-9	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response Plans, Business Continuity Plans, Disaster Recovery Plans, and Incident Handling Plans are identified, documented, communicated and managed
86	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.IP-10	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Plans identified in PR.IP-9 are exercised according to the cybersecurity risk management strategy
87	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.IP-11	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the human resources practices for on-boarding, off-boarding, privilege management are identified, documented and managed

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
88	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		Maintenance (MA)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure practices for the maintenance and repair of system components is performed consistent with identified, documented and communicated policies and procedures
89	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.MA-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the maintenance and repair of assets is documented and approved
90	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.MA-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the remote maintenance is performed consistent with PR.AC-3
91	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		Protective Technology (PT)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
92	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.PT-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the audit log retention requirements are identified and documented to support the Detect and Respond Functions and in accordance with the cybersecurity risk management strategy
93	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.PT-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical and logical ports of assets are managed according to the cybersecurity risk management strategy
94	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.PT-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical and logical access to assets are managed according to the cybersecurity risk management strategy

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
95	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	21		PR.PT-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the communication network connections are secured according to the cybersecurity risk management strategy
96	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		Anomalies and Events (AE)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure potential impacts associated with anomalous communication is detected in a timely manner to support the Respond Function
97	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.AE-2	This requirement does not appear to be different from ID.AM-3.	Remove this requirement.
98	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.AE-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detected cybersecurity events are analyzed to understand attack targets and methods
99	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.AE-3	Wonder if this should tie back to ISAC?	For critical infrastructure, the data associated with cybersecurity events is correlated from diverse information sources
100	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.AE-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detected cybersecurity events are analyzed to determine their impacts
101	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.AE-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the alerts to support incident handling and the Respond Function are identified, documented and managed according to the cybersecurity risk management strategy

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
102	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		Security Continuous Monitoring (CM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure assets are continuously monitored to identify cybersecurity events and to verify the effectiveness of the Protect Function measures.
103	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.CM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the communication networks are continuously monitored to detect potential cybersecurity events according to the cybersecurity risk management strategy
104	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.CM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical environment is continuously monitored to detect potential cyber-physical events according to the cybersecurity risk management strategy
105	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.CM-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the personnel activity is continuously monitored to detect potential cybersecurity events according to the risk management strategy
106	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	22		DE.CM-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the methods to detect malicious code are identified, documented and managed
107	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.CM-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the methods to detect mobile code are identified, documented and managed
108	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.CM-6	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	critical infrastructure, the methods to monitor external service providers are identified, documented and managed

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
109	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.CM-7	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	NOT SURE WHAT RESOURCES THIS REFERS TO? - application processes? People?
110	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.CM-8	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity vulnerability assessments are performed according to the cybersecurity risk management strategy
111	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		Detection Processes (DP)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events
112	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.DP-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity personnel roles and responsibilities for detection are identified, documented, communicated and managed
113	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.DP-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detection activities comply with legal, regulatory, privacy and civil liberties requirements
114	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.DP-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detection activities are identified, documented, exercised and managed
115	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.DP-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detected cybersecurity event information is communicated as part of identified and documented information sharing practices

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
116	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	23		DE.DP-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detection processes are continuously improved according to the cybersecurity risk management strategy
117	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		Response Plan (RP)	Removed "and tested" because PR.IP-10 did the exercising of the Plans. Also change the name of the Category to "Response Plan" since the "planning" actually also occurred in the Protect Function.	The critical infrastructure response processes and procedures are implemented to ensure timely response of detected cybersecurity events
118	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.RP-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response Plans maintained in PR.IP-10 are implemented during or after a detected cybersecurity event
119	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		Communications (CO)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure response activities are coordinated with internal and external stakeholders to include external support from federal, state and local law enforcement
120	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.CO-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the personnel roles and responsibilities for reporting cybersecurity events are identified, documented, communicated and managed
121	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.CO-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the requirements for reporting detected cybersecurity events are identified, documented, communicated and managed
122	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.CO-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity, privacy and civil liberties detection, response, and breach reporting requirements are identified, documented, communicated and managed according to the Response Plans created in PR.IP-10

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
123	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.CO-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the coordination with internal and external stakeholders (e.g. business partners, information sharing and analysis centers, government entities) includes cybersecurity, privacy and civil liberties considerations in accordance with Response Plans created in PR.IP-10
124	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.CO-5	Included this language in RS.CO-4	Remove this requirement.
125	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		Analysis (AN)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure establishes regular analysis of cybersecurity detection capabilities to support the Response and Recovery Functions.
126	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.AN-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the alerts and notifications from cybersecurity detection systems are investigated according to the risk management strategy
127	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.AN-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the impacts of a cybersecurity incident are analyzed, documented and communicated
128	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	24		RS.AN-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the analysis of evidence associated with a cybersecurity incident includes internal or external forensic analysis according to the cybersecurity risk management strategy
129	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RS.AN-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity incidents are classified consistent with the Response Plans created in PR.IP-10

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
130	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		Mitigation (MI)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure activities for mitigating a cybersecurity incident are performed to prevent expansion of an event, mitigate its effects and eradicate the incident
131	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RS.MI-1	Possibly this should be a requirement in the PR.IP-10 as an element of the Response Plans or in the RP category of Response?	For critical infrastructure, the Response Plans are implemented to contain the expansion of a cybersecurity incident
132	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RS.MI-2	Possibly this should be a requirement in the PR.IP-10 as an element of the Response Plans or in the RP category of Response?	For critical infrastructure, the Response Plans are implemented to eradicate expansion and exposure of a cybersecurity incident
133	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		Improvements (IM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure response activities are improved by incorporating lessons learned from exercising the Response Plans or from actual detected cybersecurity incidents
134	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RS.IM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response Plans from PR.IP-10 incorporate lessons learned from exercising the Response Plans or from actual detected cybersecurity incidents
135	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RS.IM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response plans from PR.IP-10 are updated from exercising the Response Plans or from actual detected cybersecurity incidents
136	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		Recovery Plan (RP)	Removed "tested" because PR.IP-10 did the exercising of the Plans. Also change the name of the Category to "Response Plan" since the "planning" actually also occurred in the Protect Function.	The critical infrastructure recovery processes and procedures are implemented to ensure timely response of detected cybersecurity events

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
137	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RC.RP-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Recovery Plans maintained in PR.IP-10 are implemented during or after a detected cybersecurity event
138	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		Improvements (IM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure recovery activities are improved by incorporating lessons learned from exercising the Response Plans or from actual detected cybersecurity incidents
139	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RC.IM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Recovery Plans from PR.IP-10 incorporate lessons learned from exercising the Response Plans or from actual detected cybersecurity incidents
140	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RC.IM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response plans from PR.IP-10 are updated from exercising the Response Plans or from actual detected cybersecurity incidents
141	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		Communications (CO)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure recovery activities are coordinated with internal and external stakeholders to include external support from federal, state and local law enforcement, information sharing and analysis centers, CSIRTs, vendors, etc.
142	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	25		RC.CO-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the requirements for managing public relations and reputation are identified, documented, communicated and managed
143	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	36	497	App C	Unclear how these areas became high priority, suggest that they are more potential areas for improvement that have been listed and described.	delete "high-priority," replace with "potential"

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
144	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	36	498	App C	How these were "identified" is unclear, suggest edits to be consistent with these areas are a discussion starting point, more work needs to be done.	replace "currently identified" with "listed and discussed below."
145	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		E	36	498	App C		change "These initial" to "The following"
146	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	36	498	App C	A list and description is not really a roadmap, but a starting point for discussion.	change "roadmap" to "discussion starting point"
147	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	36	509-516	App C	This discussion is premature, the existing framework needs to be tested first, then a more informed process to develop areas for improvement should come out of the Sector-Specific Agencies through the Sector Coordinating Councils	delete "but these highlighted…addressing the challenges."
148	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	36	518-522	App C	Prescriptive discussion, should be sector-specific and not in the NIST Framework.	delete "As a result, …such as a biometric."
149	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	38	576-584	App C	This is not an exhaustive list, sector-specific efforts are underway that are not included here, which can be confusing to the reader, lines 568-574 are adequate to address the area.	delete lines 576-584
150	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	38-39	616-617	App C	Appendix B's scope is too large, should be focused on critical infrastructure cybersecurity activities.	delete "including the Privacy Methodology in Appendix B."

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
151	Tacoma Public Utilities (representing 5 Critical Infrastructure Sectors)		T	39	617-626	App C	A detailed description of the shortcomings of the FIPPs is not needed here, get to the gap.	delete "Although the FIPPs…Privacy Methodology is limited." add "However, the FIPPs do not provide best practices and metrics for implementing privacy protections." delete "lack of standardization, and supporting privacy metrics,"