Comments template for Preliminary
Cybersecurity Framework

Submitted by: _Dan Schmelling_
Date: ___12/4/2013___________

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	EPA	Dan Schmelling	G	1-12		1,2,3	The document should provide a concise Executive Summary and otherwise eliminate the significant redundancy in sections 1-3.	Make Section 1 an Executive Summary, and combine Sections 2 and 3 into a description of how to use the Framework.
2	EPA	Dan Schmelling	G, T	3		1.2	Section 1.2 should be struck and replaced with a more robust description of risk management in Section 3.2. Currently, Section 3.2 lists the right general steps for using the framework, but provides too little guidance to users on how to carry out these steps. In particular, Section 3.2 should provide more information on assessing the relative importance of cyber threats as part of an all-hazards risk assessment (step 3) and the process of prioritizing cyber security gaps (step 5) given the high uncertainty of cost/benefit analysis and risk estimates (e.g., realistically, how should organizations determine what to do first).	Replace section 1.2 with a more robust and actionable description in Section 3.2 of how organizations should assess cyber risks as part of an overall risk assessment, and how they can appropriately prioritize activities to reduce cyber risks.

E
Type: E - Editorial, G - General T - Technical

3	EPA	Dan Schmelling	G, T	6	227-228	2.1	The description of subcategories in Section 2.1 states that they "*are not intended to be a comprehensive set of practices to support a category*." Why not? They should be. The categories should be written tightly enough that they can be supported by a set of subcategories which, if fully implemented, would achieve the category outcome. If the current subcategories don't collectively achieve a category outcome, then either the category needs to be revised, or the subcategories should be expanded, or both.	Ensure that for every category, full implementation of the subcategories will achieve the category outcome. Then revise this sentence in section 2.1 accordingly.
4	EPA	Dan Schmelling	G, T	7	281-302	2.2	This description of framework profiles in Section 2.2 should be struck as a stand alone section and incorporated into a more robust description in Section 3.2 of how to use the framework. The profile concept is useful, but only in the context of the larger risk management and prioritization process as described, albeit minimally, in Section 3.2. Users would benefit by seeing all the steps in 3.2 explained more fully, rather than having one separate preceding section that only addresses profiles.	Incorporate Section 2.2 into a more robust Section 3.2.
5	EPA	Dan Schmelling	G	8-9	307-320	2.3	The description of the notional flow of information and decisions in an organization in Section 2.3 should be struck entirely. It serves no useful role and will deter some users whose organizations don't fit this model. Organizations know how they operate and there is no reason for the framework to tell them how they make and implement decisions.	Strike section 2.3.

6	EPA	Dan Schmelling	G	9-11	321-389	2.4	The concept of framework implementation tiers is counterproductive. Section 2.4 should be modified to describe only the characteristics of a desired end state for a cybersecurity program (Tier 4). Organizations should determine a prioritized list of actions to reduce cybersecurity risk through a risk assessment, as described in Section 3.2. Imposing the selection of an implementation tier into this process is a confusing and unnecessary hurdle. Further, no organization will want to assign a low tier to its efforts.	Drop the concept of selecting an implementation tier in Section 2.4, and replace it with a description of the characteristics of a robust cybersecurity program, as listed for Tier 4.
7	EPA	Dan Schmelling	G	13-26	466	Framework Core	There are two general problems with the Framework Core: (1) There is significant redundancy among categories and subcategories. Each subcategory should comprise an activity that is fully distinct from the activities in other subcategories. (2) The framework categories and subcategories should comprise activities specific to a cybersecurity program. Currently, many of the categories and subcategories would involve all of an organizations assets, systems, operations, etc., much of which are outside the scope of a cybersecurity program. Asking organizations to "implement the Framework" will be problematic if the Framework is written to cover far more than cybersecurity.	(1) The Framework authors should revise the document to ensure that each category and subcategory is necessary and fully distinct from all the other categories and subcategories. (2) Activities in the categories and subcategories should be defined so that they are specific to cybersecurity and do not encompass general operations and management.

8	EPA	Dan Schmelling	G	13	466	ID-Asset Management	The description of asset management should be specific to cybersecurity, rather than the current general definition of asset management, which critical infrastructure organizations already practice and is beyond the scope of a cybersecurity program. Further, the associated subcategories for asset management do not collectively achieve this general category outcome (for example, no subcategories address facility or personnel management). However, the subcategories could, and should, be written to achieve an asset management outcome specific to cybersecurity.	Revise the Asset Management category to be specific to cybersecurity.
9	EPA	Dan Schmelling	G	13	466	ID.AM-1	This subcategory should be specific to devices and systems related to cybersecurity, rather than all physical devices and systems within the organization. The current general definition is outside the scope of a cybersecurity program and inconsistent with other asset management subcategories that are specific to cybersecurity.	Revise ID.AM-1 to be specific to devices and systems related to IT and ICS.
10	EPA	Dan Schmelling	G	14	466	ID.AM-6	Should refer to roles and responsibilities for cybersecurity only.	Revise to be specific to roles and responsibilities for cybersecurity.
11	EPA	Dan Schmelling	G	14	466	ID.BE-1	"supply chain" in this context should be defined.	Revise to clarify what "role in the supply chain" should encompass.
12	EPA	Dan Schmelling	G	14	466	ID.BE-2	"*Place in critical infrastructure and their industry ecosystem*" is the kind of vague terminology that will leave some users shaking their heads. Moreover, ID.BE-3 refers to organizational mission, objectivities, and activities, while ID.BE-4 covers dependencies and critical functions. These should address anything intended to be captured by "industry ecosystem".	Strike this subcategory or define the terminology if it's really needed.

13	EPA	Dan Schmelling	T	15	466	Governance	ID.GV-4 "Governance and risk management processes address cybersecurity risks" is inclusive of ID.GV-1 and 2, which address information security policy roles and responsibilities. A better approach would be to continue the more specific subcategories, like ID.GV-1&2, with additional subcategories that address other aspects of governance for cyber risks, such as industrial control systems. A very general subcategory like ID.GV-4 does little more than restate the governance category.	Replace ID.GV-4 with subcategories that address aspects of governance that are in addition to information security.
14	EPA	Dan Schmelling	T	16	466	ID.RA-5	Identifying risk responses should be under the Risk Management category, rather than the Risk Assessment category. Further, the distinction between this subcategory and ID.RM-1 "Risk management processes are managed" is unclear.	Move ID.RA-5 under Risk Management and consider consolidating with ID.RM-1.
15	EPA	Dan Schmelling	G	18, 19	466	PR.DS-3 & 7	The Data Security category addresses only information and records, whereas these subcategories address asset management generally. These subcategories should be moved and covered under the existing Asset Management category.	Address the activities covered by these subcategories in the Asset Management category.
16	EPA	Dan Schmelling	G	18	166	Information Protection Processes and Procedures	Much of this category appears to be redundant with other categories in the framework, including Asset Management, Data Security, and Response Planning.	Consider whether this entire category could be incorporated into other framework categories in an effort to tighten up the framework core. For example, PR.IP-1&2 (create a baseline configuration of IT systems and implement a system development lifecycle) should be covered under Asset Management; PR.IP-4-8 are Data Security functions; and PR.IP-9&10 are Response Planning.

17	EPA	Dan Schmelling	G	21	466	PR.MA-1&2	By including maintenance of all organizational assets in these definitions (category includes all operational system components), they encompass maintenance far beyond the scope of cybersecurity.	Limit definition to IT and ICS components.
18	EPA	Dan Schmelling	G	21	466	Protective Technology	Restrict this and corresponding subcategory definitions to assets and systems related to cybersecurity.	Limit definitions to cybersecurity
19	EPA	Dan Schmelling	G	21	466	Protective Technology	Most of this category appears redundant with earlier categories. For example, PR.PT-3, "Access…is controlled" is clearly redundant with the category of "Access Control". PR.PT-2, protecting removable media, and PR.PT-4, securing communication networks, should be covered under "Data Security".	Consider eliminating this category and ensuring that its subcategories are covered by earlier categories, as they appear to be.
20	EPA	Dan Schmelling	T	23	466	DE.CM-8	Vulnerability Assessment in this definition should be distinguished from the vulnerability assessment in ID.RA-1.	Clarify what is intended for the vulnerability assessment under continuous monitoring.
21	EPA	Dan Schmelling	G	23	466	Detection Processes	Definition should be clarified so that "Anomalous events" is specific to cybersecurity issues. Most anomalous events in most organizations aren't related to cyber.	Clarify the category and associated subcategory definitions to be specific to cybersecurity.
22	EPA	Dan Schmelling	T	24	466	RS.CO-1	"Personnel know their roles…" should be under the "Response Planning" category, or perhaps "Awareness and Training" rather than Communications	Move RS.CO-1 to Response Planning, or revise the subcategory description if this activity is intended to involve communications.
23	EPA	Dan Schmelling	G	25	466	Recovery Planning	RC.RP-1 is the execution of a Recovery Plan, but no subcategory explicitly involves the development of a recovery plan for a cyber incident.	Add a subcategory that addresses the development of recovery plans for a cyber incident.