Submitted by: <u>Dan Schmelling</u>
Date: <u>12/4/2013</u>

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.
						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	
						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	
						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	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.
		1 EPA Dan Schmelling	1 EPA Dan Schmelling G	1 EPA Dan Schmelling G 1-12	1 EPA Dan Schmelling G 1-12	1 EPA Dan Schmelling G 1-12 1,2,3	# Comment) The document should provide a concise Executive Summary and otherwise eliminate the significant redundancy in sections 1-3. 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

Submitted by: <u>Dan Schmelling</u>
Date: <u>12/4/2013</u>

							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	Ensure that for every category, full implementation of the subcategories will
								achieve the category outcome. Then revise this
3	EPA	Dan Schmelling	G, T	6	227-228	2.1	be expanded, or both.	sentence in section 2.1 accordingly.
		•					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	Incorporate Section 2.2 into a more robust
4	EPA	Dan Schmelling	G, T	7	281-302	2.2	addresses profiles.	Section 3.2.
		-					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	
5	EPA	Dan Schmelling	G	8-9	307-320	2.3	implement decisions.	Strike section 2.3.

							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	Drop the concept of selecting an implementation tier in Section 2.4, and replace it with a description of the characteristics of a robust
6	EPA	Dan Schmelling	G	9-11	321-389	2.4	assign a low tier to its efforts.	cybersecurity program, as listed for Tier 4.
							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	(1) The Framework authors should revise the
								document to ensure that each category and
							of a cybersecurity program. Asking	all the other categories and subcategories. (2)
							organizations to "implement the	Activities in the categories and subcategories
							Framework" will be problematic if the	should be defined so that they are specific to
						Framewor	Framework is written to cover far more	cybersecurity and do not encompass general

than cybersecurity.

7 EPA

Submitted by: _Dan Schmelling_

Date: ___12/4/2013_

operations and management.

Dan Schmelling G

13-26

466 k Core

Submitted by: <u>Dan Schmelling</u>
Date: <u>12/4/2013</u>

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 could, and is specific to device and should, be written to achieve an asset Managemen management countries address facility or personnel management). However, the subcategories could, and is should, be written to achieve an asset Managemen management countries and the cybersecurity. However, the subcategories could, and is should, be written to achieve an asset Managemen management countries and should, be written to achieve an asset Management category to be specific to devices and systems related to cybersecurity. The current general definition is outside the scope of a cybersecurity management subcategories that are specific to eybersecurity. The current general definition is outside the scope of a cybersecurity management subcategories that are specific to eybersecurity. Should refer to roles and responsibilities for cybersecurity. Should refer to roles and responsibilities for cybersecurity. Place in critical infrastructure and theti-industry ecosystems 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" considerations.								The description of asset management	
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 Manageme management outcome specific to device and should, be written to achieve an asset Management outcome specific to devices and systems related to cybersecurity. See PA Dan Schmelling G 13 466 ID.AM-1 This subcategory should be specific to devices and systems within the organization. The current general definition is outside the scope of a cybersecurity. The train 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 devices and systems related to IT and ICS. Should refer to roles and responsibilities for cybersecurity. PEPA Dan Schmelling G 14 466 ID.AM-6 ID.BE-1 "Flace 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									
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 to achieve an asset management on the companies of the cybersecurity. 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 organ and inconsistent with other asset management subcategories that are specific to cybersecurity. 9 EPA Dan Schmelling G 13 466 ID.AM-1 cybersecurity. 10 EPA Dan Schmelling G 14 466 ID.BE-1 for cybersecurity organ and inconsistent with other asset management subcategories that are specific to cybersecurity. Revise to Dan Schmelling G 14 466 ID.BE-1 in this context should be defined. 11 EPA Dan Schmelling G 14 466 ID.BE-1 regional for cybersecurity organ and inconsistent with other asset management subcategories that are specific to recybersecurity. Revise to clarify what "role in the supply chain" in this context should be defined. 12 EPA Dan Schmelling G 14 466 ID.BE-1 regional first inclusive, while ID.BE-3 refers to organizational mission, objectivities, and activities, while ID.BE-4 covers dependencies and critical functions. These should address anything									
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 Manageme management outcome specific to devices and systems related to cybersecurity. 8 EPA Dan Schmelling G 13 466 nt cybersecurity. This subcategory should be specific to devices and systems related to cybersecurity. 9 EPA Dan Schmelling G 13 466 ID.AM-1 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. 9 EPA Dan Schmelling G 14 466 ID.AM-1 cybersecurity. 10 EPA Dan Schmelling G 14 466 ID.AM-6 for cybersecurity. 11 EPA Dan Schmelling G 14 466 ID.BE-1 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									
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 Manageme management outcome specific to cybersecurity. 8 EPA Dan Schmelling G 13 466 nt cybersecurity, rather than all physical 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 success and systems related to Cybersecurity. Should refer to roles and responsibilities for cybersecurity. 9 EPA Dan Schmelling G 14 466 ID.AM-1 (cybersecurity) only. 10 EPA Dan Schmelling G 14 466 ID.AM-1 (cybersecurity). 11 EPA Dan Schmelling G 14 466 ID.BM-1 (cybersecurity) only. 12 Supply chain" in this context should be defined. 13 Flace 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									
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 Manageme should, be written to achieve an asset management outcome specific to cybersecurity. BEPA Dan Schmelling G 13 466 nt cybersecurity. This subcategory should be specific to cybersecurity. This subcategory should be specific to cybersecurity. This subcategory should be specific to cybersecurity. The current general definition is outside the scope of a cybersecurity program and inconsistent with other asset management subcategories that are specific to cybersecurity. Should refer to roles and responsibilities for cybersecurity. Should refer to roles and responsibilities for cybersecurity. Revise to be specific to devices and systems related to IT and ICS. Should refer to roles and responsibilities for cybersecurity. Revise to be specific to roles and responsibilities for cybersecurity. Revise to be specific to roles and responsibilities for cybersecurity. Revise to be specific to roles and responsibilities for cybersecurity. Revise to derify what "role in the supply chain" should encompass. Revise to derify what "role in the supply chain" should encompass. Revise to derify what "role in the supply chain" should encompass. Revise to derify what "role in the supply chain" should encompass. Revise to derify what "role in the supply chain" should encompass. Revise to derify what "role in the supply chain" should encompass. Revise to derify what "role in the supply chain" should encompass. Revise to derify what "role in the supply chain" should encompass.									
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 management outcome specific to eybersecurity. 8 EPA Dan Schmelling G 13 466 Int eybersecurity. This subcategory should be specific to devices and systems related to eybersecurity, 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 eybersecurity. 9 EPA Dan Schmelling G 13 466 ID.AM-1 cybersecurity. Should refer to roles and responsibilities for cybersecurity. 10 EPA Dan Schmelling G 14 466 ID.AM-6 for cybersecurity only. Should refer to roles and responsibilities for cybersecurity. 11 EPA Dan Schmelling G 14 466 ID.BE-1 defined. "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 organization in mission, objectivities, and activities, while ID.BE-4 covers dependencies and critical functions. These should address anything									
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 expersecurity. This subcategory should be specific to devices and systems related to cybersecurity, rathen 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 experse specific to 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 systems related to IT and ICS. Should refer to roles and responsibilities for cybersecurity. Pace 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									
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 eybersecurity. BEPA Dan Schmelling G 13 466 nt eybersecurity. This subcategory should be specific to devices and systems related to eybersecurity, rather than all physical devices and systems within the organization. The current general definition is outside the scope of a eybersecurity program and inconsistent with other asset management subcategories that are specific to eybersecurity. PEPA Dan Schmelling G 13 466 ID.AM-1 eybersecurity. Should refer to roles and responsibilities for eybersecurity only. Should refer to roles and responsibilities for eybersecurity. Should refer to roles and responsibilities for eybersecurity. 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 drives anything									
example, no subcategories address facility or personnel management). However, the subcategories could, and should, be written to achieve an asset Management category to be specific to cybersecurity. 8 EPA Dan Schmelling G 13 466 nt cybersecurity 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 systems related to IT and ICS. 8 EPA Dan Schmelling G 13 466 ID.AM-1 (cybersecurity program and inconsistent with other asset management subcategories that are specific to systems related to IT and ICS. 8 EVA Dan Schmelling G 14 466 ID.AM-6 (cybersecurity only. Should refer to roles and responsibilities for cybersecurity only. "supply chain" in this context should be defined. 10 EPA Dan Schmelling G 14 466 ID.BE-1 (rifical 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									
facility or personnel management). However, the subcategories could, and should, be written to achieve an asset management outcome specific to cybersecurity. 8 EPA Dan Schmelling G 13 466 nt cybersecurity in 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 eybersecurity only. PEPA Dan Schmelling G 13 466 ID.AM-1 cybersecurity only. Should refer to release the Asset Management category to be specific to devices and systems related to cybersecurity. Revise ID.AM-1 to be specific to devices and systems related to IT and ICS. Should refer to roles and responsibilities for cybersecurity only. "supply chain" in this context should be defined. "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									
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. This subcategory should be specific to cybersecurity. This cybersecurity. This subcategory should be specific to cybersecurity. This cybersecurity. This subcategory should be specific to cybersecurity. This cybersecurity. This cybersecurity. This cybersecurity. This cybersecurity. This cybersecurity. The current general definition is outside the scope of a cybersecurity. The cybersecurity of a cybersecurity. This cybersecurity. The cybersecurity. The current general definition is outside the scope of a cybersecu									
BEPA Dan Schmelling G 13 466 nt cybersecurity.									
Manageme management outcome specific to cybersecurity. This subcategory should be specific to devices and systems related to cybersecurity, rather than all physical definition is outside the scope of a cybersecurity method and inconsistent with other asset management subcategories that are specific to experience and systems related to cybersecurity program and inconsistent with other asset management subcategories that are specific to experse curity. PEPA Dan Schmelling G 13 466 ID.AM-1 cybersecurity. Should refer to roles and responsibilities for cybersecurity. "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							ID-Asset		
8 EPA Dan Schmelling G 13 466 nt cybersecurity. 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 evices and systems related to Trand ICS. Should refer to roles and responsibilities for cybersecurity. PEPA Dan Schmelling G 14 466 ID.AM-1 Dan Schmelling G 14 466 ID.BE-1 This subcategory should be specific to devices and systems related to Trand ICS. Revise ID.AM-1 to be specific to devices and systems related to IT and ICS. Should refer to roles and responsibilities for cybersecurity. Should refer to roles and responsibilities for cybersecurity. Revise to be specific to roles and responsibilities for cybersecurity. Revise to clarify what "role in the supply chain" should be defined. "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									Revise the Asset Management category to be
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 evices and systems related to IT and ICS. Should refer to roles and responsibilities for cybersecurity only. BPA Dan Schmelling G 14 466 ID.AM-6 for cybersecurity only. BPA Dan Schmelling G 14 466 ID.BE-1 defined. BPA Dan Schmelling G 15 Ade ID.AM-1 to be specific to devices and severity. BPA Dan Schmelling G 15 Ade ID.AM-1 to be specific to devices and severity program and inconsistent with other asset management subcategories that are specific to devices and severity. BPA Dan Schmelling G 18 Ade ID.AM-1 to be specific to devices and severity program and inconsistent with other asset management subcategories that are specific to expecific to devices and severity program and inconsistent with other asset	8	EPA	Dan Schmelling	G	13				
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 systems related to IT and ICS. Should refer to roles and responsibilities for cybersecurity. Beyon Dan Schmelling G 14 466 ID.AM-6 ID.AM-6 ID.AM-1 in this context should be defined. The program of the supply chain in this context should be defined. The program and inconsistent with other asset management subcategories that are specific to gybersecurity. Should refer to roles and responsibilities for cybersecurity. Revise to be specific to roles and responsibilities for cybersecurity. The program and inconsistent with other asset management subcategories that are specific to gybersecurity. Should refer to roles and responsibilities for cybersecurity. The program and inconsistent with other asset management subcategories that are specific to order and incompass. The program and inconsistent with other asset management subcategories that are specific to oles and responsibilities for cybersecurity. The program and inconsistent with other asset management subcategories that are specific to oles and responsibilities for cybersecurity. The program and inconsistent with other asset management subcategories that are specific to oles and responsibilities for cybersecurity. The program and inconsistent with other asset management subcategories that are specific to oles and responsibilities for cybersecurity only. The program and inconsistent with other asset management subcategories that are specific to oles and responsibilities for cybersecurity. The program and inconsistent with other asset management subcategories that are specific to oles and responsibilities for cybersecurity. The program and inconsistent with other asset management subcategories that are specific to oles in the cybersecurity. The program and inconsistent with oth									
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 systems related to IT and ICS. Per Dan Schmelling G 14 466 ID.AM-6 (cybersecurity). Should refer to roles and responsibilities for cybersecurity only. Dan Schmelling G 14 466 ID.BE-1 "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									
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. PEPA Dan Schmelling G 13 466 ID.AM-1 cybersecurity. Dan Schmelling G 14 466 ID.AM-6 for cybersecurity only. Dan Schmelling G 14 466 ID.BE-1 defined. 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									
organization. The current general definition is outside the scope of a cybersecurity program and inconsistent with other asset management subcategories that are specific to evices and systems related to IT and ICS. Dan Schmelling G 14 466 ID.AM-1 Should refer to roles and responsibilities for cybersecurity. Dan Schmelling G 14 466 ID.BE-1 Should refer to roles and responsibilities for cybersecurity. Dan Schmelling G 14 466 ID.BE-1 "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									
cybersecurity program and inconsistent with other asset management subcategories that are specific to systems related to IT and ICS. Should refer to roles and responsibilities for cybersecurity. Page 10 EPA Dan Schmelling G 14 466 ID.AM-6 for cybersecurity only. Should refer to roles and responsibilities for cybersecurity. Revise to be specific to roles and responsibilities for cybersecurity. Revise to clarify what "role in the supply chain" in this context should be defined. "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									
with other asset management subcategories that are specific to cybersecurity. Dan Schmelling G 13 466 ID.AM-1 cybersecurity. Dan Schmelling G 14 466 ID.AM-6 for cybersecurity only. Dan Schmelling G 14 466 ID.BE-1 Dan Schmelling G 14 466 ID.BE-1 EPA Dan Schmelling G 14 466 ID.BE-1 Dan Schmelling G 14 466 ID.BE-1 Should refer to roles and responsibilities for cybersecurity only. "supply chain" in this context should be defined. "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								definition is outside the scope of a	
9 EPA Dan Schmelling G 13 466 ID.AM-1 cybersecurity. 10 EPA Dan Schmelling G 14 466 ID.AM-6 for cybersecurity only. 11 EPA Dan Schmelling G 14 466 ID.BE-1 subcategories that are specific to roles and responsibilities for cybersecurity only. 12 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								cybersecurity program and inconsistent	
9 EPA Dan Schmelling G 13 466 ID.AM-1 cybersecurity. Systems related to IT and ICS. 10 EPA Dan Schmelling G 14 466 ID.AM-6 for cybersecurity only. Should refer to roles and responsibilities for cybersecurity. 11 EPA Dan Schmelling G 14 466 ID.BE-1 should refer to roles and responsibilities for cybersecurity. 12 EPA Dan Schmelling G 14 466 ID.BE-1 defined. 13 EPA Dan Schmelling G 14 466 ID.BE-1 should refer to roles and responsibilities for cybersecurity. 14 EPA Bar Schmelling G 14 466 ID.BE-1 defined. 15 EPA Dan Schmelling G 14 466 ID.BE-1 defined. 16 EPA Dan Schmelling G 14 466 ID.BE-1 defined. 17 EPA Bar Schmelling G 14 466 ID.BE-1 defined. 18 EPA Dan Schmelling G 14 466 ID.BE-1 defined. 19 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								with other asset management	
Should refer to roles and responsibilities for cybersecurity. Revise to be specific to roles and responsibilities for cybersecurity. Revise to be specific to roles and responsibilities for cybersecurity. Revise to clarify what "role in the supply chain" should encompass. 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								subcategories that are specific to	Revise ID.AM-1 to be specific to devices and
10 EPA Dan Schmelling G 14 466 ID.AM-6 for cybersecurity only. for cybersecurity. 11 EPA Dan Schmelling G 14 466 ID.BE-1 defined. 12 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	9	EPA	Dan Schmelling	G	13	466	ID.AM-1		
"supply chain" in this context should be defined. Dan Schmelling G 14 466 ID.BE-1 "supply chain" in this context should be defined. "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								Should refer to roles and responsibilities	Revise to be specific to roles and responsibilities
11 EPA Dan Schmelling G 14 466 ID.BE-1 defined. should encompass. "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	10	EPA	Dan Schmelling	G	14	466	ID.AM-6		
"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									
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	11	EPA	Dan Schmelling	G	14	466	ID.BE-1		should encompass.
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									
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									
refers to organizational mission, objectivities, and activities, while ID.BE- 4 covers dependencies and critical functions. These should address anything									
objectivities, and activities, while ID.BE- 4 covers dependencies and critical functions. These should address anything									
4 covers dependencies and critical functions. These should address anything									
functions. These should address anything									
intended to be captured by "industry Strike this subcategory or define the									
12 EPA Dan Schmelling G 14 466 ID.BE-2 ecosystem". terminology if it's really needed.	12	EPA	Dan Schmelling	G	14	466	ID.BE-2	ecosystem".	terminology if it's really needed.

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

							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	Replace ID.GV-4 with subcategories that
4.0		5 61 11					more than restate the governance	address aspects of governance that are in
13	EPA	Dan Schmelling	T	15	466	e	category.	addition to information security.
							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	
							e ;	Move ID.RA-5 under Risk Management and
14	EPA	Dan Schmelling	Т	16	466	ID.RA-5	unclear.	consider consolidating with ID.RM-1.
	2111	2 wii 2 ciiii ciiii g		10		12.10.10	The Data Security category addresses	Constant Consonauxing with 12 12 12
							only information and records, whereas	
							these subcategories address asset	
							management generally. These	
							subcategories should be moved and	Address the activities covered by these
						PR.DS-3	covered under the existing Asset	subcategories in the Asset Management
15	EPA	Dan Schmelling	G	18, 19	466	& 7	Management category.	category.
								Consider whether this entire category could be
								incorporated into other framework categories in
						T. C		an effort to tighten up the framework core. For
						Informatio	3.6 1 Cd.: 4	example, PR.IP-1&2 (create a baseline
				l			Much of this category appears to be	configuration of IT systems and implement a
							redundant with other categories in the	system development lifecycle) should be
						Processes	framework, including Asset	covered under Asset Management; PR.IP-4-8
1.0	EPA	Dan Schmelling	C	18		Processes and		

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

				By including maintenance of all	
				organizational assets in these definitions	
				(category includes all operational system	
				components), they encompass	
			PR.MA-	maintenance far beyond the scope of	
17 EPA	Dan Schmelling G	21	466 1&2	cybersecurity.	Limit definition to IT and ICS components.
1/EIA	Dan Schmennig G	21		Restrict this and corresponding	I and ics components.
18 EPA	Dan Schmelling G	21	466 v	systems related to cybersecurity.	Limit definitions to cybersecurity
TOLFA	Dan Schinening G	21	400 y	systems related to cybersecurity.	l Chilit definitions to cybersecurity
				Most of this category appears redundant	
				with earlier categories. For example,	
				PR.PT-3, "Accessis controlled" is	
				clearly redundant with the category of	
				"Access Control". PR.PT-2, protecting	
			Protective		Consider eliminating this category and ensuring
				communication networks, should be	that its subcategories are covered by earlier
19 EPA	Dan Schmelling G	21		covered under "Data Security".	
19 EPA	Dan Schmelling G	21	466 y	Vulnerability Assessment in this	categories, as they appear to be.
				definition should be distinguished from	Clarify what is intended for the walnesshility
20 EPA	Dan Sahmallina T	23	466 DE.CM-8	the vulnerability assessment in ID.RA-1.	Clarify what is intended for the vulnerability assessment under continuous monitoring.
20 EPA	Dan Schmelling T	23	400 DE.CM-8	Definition should be clarified so that	assessment under continuous monitoring.
				"Anomalous events" is specific to	
			_D , ,	cybersecurity issues. Most anomalous	
21 ED4			Detection	events in most organizations aren't	Clarify the category and associated subcategory
21 EPA	Dan Schmelling G	23	466 Processes	related to cyber.	definitions to be specific to cybersecurity.
				"Personnel know their roles" should be	
				under the "Response Planning" category,	Move RS.CO-1 to Response Planning, or revise
22 ED4	D 0 1 11: T		466 PG GG 1	or perhaps "Awareness and Training"	the subcategory description if this activity is
22 EPA	Dan Schmelling T	24	466 RS.CO-1	rather than Communications	intended to involve communications.
				RC.RP-1 is the execution of a Recovery	
				Plan, but no subcategory explicitly	Add a subcategory that addresses the
	-		Recovery	involves the development of a recovery	development of recovery plans for a cyber
23 EPA	Dan Schmelling G	25	466 Planning	plan for a cyber incident.	incident.