#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	DOD		G	0	0		DOD appreciates the opportunity to comment on the Preliminary Cybersecurity Framework and the efforts of NIST, critical infrastructure owners and operators, and other stakeholders in this consultative process.	
2	DOD		G	0	0		This Framework provides companies with existing cybersecurity programs the tools to better manage risk and inform and prioritize decisions regarding cybersecurity. However, there may also be a need to define how to establish an effective cybersecurity program for companies with a fledging program, or no program at all.	Consider adding an appendix related to establishing an effective cybersecurity program.
3	DOD		G	0	0		A threat-based approach to protecting the critical infrastructure provides a proactive rather than a reactive approach to managing cybersecurity risks. The approach documented in the Framework is a traditional, risk-based cybersecurity approach with the addition of a few threat-oriented subcategories. An active threat-based defense approach provides the opportunity to make intelligence-driven decisions.	Discuss the concepts of a cyber threat-based defense in the Introduction and have cyber threat intelligence drive execution of the core functions. Tie the outcomes/activities to a larger threat-driven approach. Explain how the information is pulled into the organization's cyber threat knowledgebase and correlated with/against existing threat and log data and used to make intelligence-driven decisions.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
4	DOD		G	1	80-81		Management of risk can be more effective when each threat and potential impact is considered prominently in the processes. Rationale: A clear understanding of the threats is also important to managing cybersecurity risk. Generally, next revision of document should address risk management using a threat-based approach.	Add “threats” to the sentence.
5	DOD		E	1	86-87		It is not clear what the larger systemic risks inherent to critical infrastructure means. Rationale: This is the only time the word systemic is used in the document. Consider modifying the sentence with additional text or removing the phrase that starts with while.	Define other larger systemic risk.
6	DOD		G	1	65	1	How does an industry know it is part of the "critical infrastructure"?	Recommend an appendix listing industries currently considered as "critical". The document needs a feedback loop for current or new organizations that believe they fit the "critical" definition so the govt can ensure they are included in this effort.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
7	DOD		T	1	83	1	The Framework does not address the cybersecurity challenges of industries or sectors as a whole, but is aimed at securing an individual enterprise. The Framework should address threat sharing, which allows and encourages organizations to address the cybersecurity needs of their industry/sector and the ecosystem of that industry/sector that they collectively represent.	In the Introduction, discuss the concept of organizations existing as part of an industry/sector ecosystem and the need to share information. Add a function to the Framework, Orient, that identifies the need to define an organization's place within the ecosystem in relationship to other organizations, or amend the Identify function to include such content.
8	DOD		T	1	70	1	Organizations need to look beyond compliance risk. In security and privacy, the default tends to be a compliance risk model, but that model can miss some of the biggest risks an organization faces.	Add language that indicates privacy compliance requirements are a “floor” not a “ceiling," and that organizations must determine how to identify privacy risks that result in harm to individuals.
9	DOD		G	1	80-81		Management of risk can be more effective when each threat and potential impact is considered prominently in the risk management process. Rationale: A clear understanding of the threats is also important to managing cybersecurity risk. Generally, next revision of document should address risk management using a threat-based approach.	Add “threats” to the sentence.
10	DOD		G	1	95-99		Five purposes are given. It is unclear who the target audience is, i.e. USG Departments and Agencies, the Private Sector, or other partners. Further it is not clear whether this document is prescriptive, directive, or suggested.	Identify target audience, legal mandate for this framework and legal standing of document (i.e.public law, the EO itself, etc.)

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
11	DOD		G	2	117-118, et al		The Framework is structured for top down risk management. Rationale: As a process, risk management works better as a holistic process of organizational behavior that includes engagement at all levels, where risk is addressed and validated above, below, across, and within the organization.	Consider major revision to this section to more tightly couple risk and consequences at all organizational levels.
12	DOD		T	3	180-183		Mention dependencies in this paragraph. Rationale: In addition to the earlier comment recommending changing the framework to a threat-centric approach to risk management in next revision, the common understanding of system and inter-system dependencies varies widely as well.	Add the word dependencies between "resources" and "risk tolerances".
13	DOD		G	5	212-213		The framework functions are useful for establishing the baseline risk management methodology at the lowest implementation tiers, but lack the robustness necessary to achieve Tier 3 or Tier 4 implementation levels. Rationale: For computer security professionals, these labels make sense, but others may lack meaningful context that will be necessary to realize the "organization-wide approach to manage cybersecurity risk". Ultimately, the goal needs to be to provide the protections necessary to improve and assure critical infrastructure.	Consider adding business system processes and operational functions necessary to delineate and address the day-to-day strategic management of risk posture at all levels in the organization.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
14	DOD		T	5	212	2.1	The Framework core should address resiliency separate from the Respond and Recover functions. While the respond and recovery functions are important, they focus on managing communications about the event and returning the organization to its original capability. Resiliency should focus on allowing an organization to continue to operate in spite of any cyber incidents. The description of Recover assumes that one is recovering from a loss of service due to an incident, but a successful incident need not equate to loss of services, simply a penetration of the perimeter.	Add a function to the Framework, Withstand, that identifies the needs of an organization to adapt to evolving threats and continue fulfilling mission essential functions throughout periods of degradation that affect an organization's own operations or that of their external stakeholders.
15	DOD		T	6	221-223		The framework needs to expand on the training, planning, and exercises in more detail. Rationale: Exercises within any function or business process are necessary in the formative stages of risk management. All of the business processes, not just those in cybersecurity, must be validated in order to assure a reliable and resilient cybersecurity posture.	Incorporate notion of organizational level exercises across business functions to include cybersecurity, not just for cybersecurity.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
16	DOD		T	6	243-251		The framework should incorporate identification of dependencies specifically. Rationale: Determining the mission essential functions and their dependencies is difficult. The hardest task is the prioritization, and only with comprehensive evaluation and exercise can this be successful. It is easier to do this early and often in the risk management implementation process.	Revise the document to address locating and understanding all of the mission essential functions and their dependencies. A process to conduct and validate the prioritization should also be discussed and incorporated into the framework.
17	DOD		G	6	224	2.1 and Glossary	The description and use of the terms category and subcategory are not consistent between their description on page 6 and their definitions in the glossary. In addition, the relationship between categories/subcategories and outcomes or activities is not clear.	Clarify the terms category, subcategory, outcome, and activities and their relationship.
18	DOD		G	9	Fig 3 318-319	2.3	Fig 3 brings together and details what have been abstract concepts and provides a good picture of the communications plan, but Fig 3 is not adequately supported by the preceding lines of explanation (310-317).	Figure 3 should be more clearly explained. There are 7 icons with titles/info - each of these should be discussed in more detail so that the reader can relate it to activities they understand.
19	DOD		T	9	322-323	2.4	Use of "Tiers" with two different meanings is confusing. In Sec 1.1, page 2, lines 111-112, Tiers are: Core, Profile, and Implementation Tiers. In Section 2.4 Tiers are: Partial (Tier 1) through Adaptive (Tier 4).	Recommend changing "Tiers" in section 1.1 to "Steps" or "Parts" to reduce confusion.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
20	DOD		G	11	404-406	3.1	The Framework needs to provide, or at least reference, a preferred standard against which to compare how an organization stacks up against a known, acceptable standard. The NIST SP 800 documents would be ideal, because they are widely used internationally and amongst the private sector.	Recommend tying this Framework more closely with NIST SP 800 documents.
21	DOD		T	11	409-436	3.2	Need more specificity in this section.	Recommend adding content to explain: - What roles are typically involved with each step? - What type of documentation usually results from each step? - Examples/case studies/more detail. We should identify activities, documentation (such as cybersecurity strategy), what roles are involved, and examples/case studies that show what this looks like. - How do companies determine their risk tolerance, or what risks are out there?
22	DOD		T	14	ID.BE-1	Table 1	SA-12 is the control focused on supply chain, it should be included in this list of references.	Include SA-12.
23	DOD		T	14	ID.BE-4	Table 1	Reconsider the selection of controls mapped to this topic. Most of the controls cited included the word "critical" somewhere in the control or supplemental guidance, but they do not all relate to the cited subcategory.	Include CP-2. Reconsider: CP-8, PE-9, PE-10, PE-11, PE-12, PE-14. These controls appear questionable.
24	DOD		T	17	PR.AC-3	Table 1	AC-19 is for mobile devices, AC-20 is related to external providers. Neither is relevant to remote access, which is the topic of this subcategory.	Remove AC-19 and 20.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
25	DOD		T	17	PR.AC-4	Table 1	AC-4 is information flow largely designed for cross domain systems. Therefore, it is not relevant to this topic. AC-16 is security attributes, only marginally related to this topic.	Remove AC-4 and AC-16.
26	DOD		T	17	PR.AC-5	Table 1	SC-8 deals with transmission confidentiality and integrity.	Include SC-8.
27	DOD		T	18	PD.DS-2	Table 1	SA-3 address the SDLC, which is closely linked to the topic of this subcategory.	Include SA-3.
28	DOD		T	19	PR.DS-5	Table 1	The focus of AU-13 is unauthorized disclosure/exfiltration. PE-3 has a control extension that deals with unauthorized exfiltration. Both appear to be appropriate to this subcategory.	Include PE-3 and AU-13.
29	DOD		T	21	PR	Table 1	ID.RA-1 States. While the need to identify and document vulnerabilities is specified in the Identify function (ID.RA-1), the need to address the identified vulnerabilities is absent in the Protect function.	Add a subcategory in the Protect, Protective Technology section that addresses the identified vulnerabilities (e.g., patching). Review the SC and SI families for possible security control mappings.
30	DOD		T	21	PR.PT-4	Table 1	SC-8 deals with transmission confidentiality and integrity.	Include SC-8.
31	DOD		G	24		Table 1	There is inconsistent terminology used within the Response Function (cyber "event" and "incident"). Response Planning and Communication talk about events while Analysis and Mitigation speak to incidents.	Recommend making clear the distinction between event (more generic) and incident (a breach/compromise has occurred, which requires specific containment/response activities). Both are of interest and should be a source of cyber threat information for the organization.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
32	DOD		T	25	RS.MI-1	Table 1	AC-4, SC-3, and SC-7 all deal with controlling the flows of data, containment, and segmentation. These are all means of containing an incident.	Include AC-4, SC-3, and SC-7.
33	DOD		G	26	469	Appen A, Informative References	Should also include in the references section 800-53A - this doc shows how to assess what has been implemented through 800-53. Note that Append B, Table 3 uses strictly SP 800 series controls as references.	Recommend including 800-53A in the references section. Anywhere 800-53 is mentioned in Appen A, 800-53A should be listed as well.
34	DOD		G	27	484	Appen A, Table 2,	Unique identifiers have already been defined in Table 1. The definitions in Table 1 are much clearer than this stand alone table 2.	Recommend deleting lines 478-484 and Table 2 as duplicative.
35	DOD		G	35	500-508	App C	Consider adding some current pressing issues that need to be addressed.	Recommend consider adding: - Removable media - Mobile devices - Insider threat - Identify Management - New technologies
36	DOD		T	38	597	C.6	NIST security controls are mapped and considerate of ISO/IEC 15408 standards already.	Recommend emphasizing in this section that being aligned internationally doesn't prevent entities from using NIST security controls.
37	DOD		G	38	622-623	C.7	Distinguishing between necessary and unnecessary is an organization by organization determination. A roadmap to assist organizations exists in Appendix J of 800-53.	This section should note that NIST SP 800-53, Appendix J. does serve as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, whether in paper or electronic form.
38	DOD		G	38	633	C.8	SCRM has been addressed by NIST, so it is more than an emerging discipline.	Recommend reviewing and referencing NIST SP 800-161 SCRM Practices, the draft of which was released for public comment 8/2013.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
39	DOD		G	42	686	Appen E	Need to ensure that all definitions are properly referenced with common taxonomy.	Highly recommend providing references for all terms in order to establish validity of definitions. If term is used only in this document, make a statement to that effect.
40	DOD		G	42	686	Glossary	Include a definition of cybersecurity in the Glossary. This term is used frequently without a consistent definition.	Recommended definition of cybersecurity as defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23: "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."
41	DOD		T	2-3	140-149		Profiles can be useful, but they generally lack the requisite flexibility to address risk in large, complex and/or mission-essential systems. Rationale: Applying profiles to systems that are not understood well or change more rapidly than the pace of risk management processes can result in scenarios where the risk posture of the system is misaligned or left vulnerable to threats that do not apply to the profile applied.	Consider major revision in future releases to go beyond the baseline level and develop a robust technical basis.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
42	DOD		G	36-39	493-645		Appendix C should identify areas for improvement in existing areas that are already implementable and achievable. Rationale: Future collaboration with particular sectors and standards organizations should also emphasize and address items that can be implemented now, but are not working as well as may have been envisioned.	Consider being more prescriptive and specific about fundamental protections and existing mitigations that could address shortfalls in the areas identified. The Framework should encourage more aggressive, rapid response and compliance for this work and the work that still needs to be done.
43	DOD		T	8-9	313-317		The notional risk management information and decision flows must acknowledge that risk decisions are made at all levels within an organization. Rationale: Final risk decisions do flow up to senior management for decision. The information usually does not account for trade space decisions regarding cybersecurity. The true impact is more likely to be well understood at implementation levels lower in the organization, which will determine the actual outcome during an event.	Discuss and depict the fact that risk decisions and impacts occur at all levels within an organization.
44	DOD		G				The framework must provide a reference implementation	Add annex with a use case to demonstrate implementation using the framework
45	DOD		G				Resiliency is not emphasized in this document. Although SP 800-53 is referenced, resiliency needs to be in the forefront in this framework. Organizations need to plan for degraded cyber conditions to avoid potential loss. This is critical to private, public and government networks.	Add resiliency information in the framework.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
46	DOD		G	0	0		This framework may be written at too high a level to be executable at the company level. NIST SP 800-37, the Risk Management Framework, is written at a level that can be executed by industry individuals not well-versed in risk management principals.	Recommend adding more detail to provide clear guidance on implementation, or add an appendix on implementing the Framework. - Need to present what a minimum, generic, risk management program should look like for a company. Without a standard for comparison, a reasonably accurate Profile cannot be developed, nor can a Target Profile be reasonably determined. - Need to point to a recommended risk assessment methodology - like a basic rendition of the 800-30 model - that is not resource intensive and can be used at the company level. - Need to identify custodialship of this document and feedback to a NIST or industry advisory group.