#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	DHS	IER Support	E		24		Will the Preliminary Framework help address gaps in cybersecurity policy and best practices within a specific sector? **Rationale: Before implementing the Preliminary Framework, organizations might want to evaluate their existing sector guidance and risk management processes against the Framework to determine what implementation is cost-beneficial and time-efficient, and leverage the Framework as supplemental cybersecurity coverage versus instituting an entirely new process.**	Within each Framework Core Function activity, it may be beneficial to suggest one or two critical activities to provide a foundation of best practices to build upon in the future.
2	DHS	NCCIC SWO / NCCIC Policy		1	80	1	Footnote 2 provides a link to a page that does not list the critical infrastructure sectors.	Recommend replacing the existing link with the following: http://www.dhs.gov/critical-infrastructure-sectors
3	DHS	Zerbi	Substantive	1	88	Introduction	EO states that the Framework should be based on "voluntary consensus standards and industry best practices to the fullest extent possible" and "consistent with voluntary international standards when such international standards will advance the objectives of this order". Nowhere in the introduction is this stated. Specially the part of **voluntary** standards. In view that the implementation of this framework is suposed to be voluntary**,** this fact should be included in the introduction.	The Framework relies on existing *voluntary* standards, guidance, and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk.
4	DHS	ISS	Administrative	1	91	1	Consistency	add "guidance and best practices" after standards

5	DHS	IER Support	G	2	104		**Add:** The Framework acts as a conduit to establish communications and foster partnerships with small, medium, and large organizations to ultimately increase cybersecurity and resilience throughout the nation.	Suggest adding in a statement about how the Framework potentially fosters new parternships with private sector organizations. The Framework acts as a conduit to establish communications and build a partnership with small, medium, and large organizations to ultimately increase cybersecurity and resilience.
6	DHS	NIC		2	114	1.1	Since the framework supports NIMS, along with other aspects of resliency, mitigation, protection, response, and recovery activties the first line should indicate broad spectrum support and applicability throughout the whole community.	Review and enhance language to include using terms that are currently used in other areas vice using "framework" repeatedly.
7	DHS	NCCIC Policy		3	163	1.2	It may be worthwhile to reference ICT as opposed to IT and ICS. EO 13636 identifies whole of nation activities, "ICT" seems a bit more contemporary.	Recommend replacing "IT and ICS assets and systems" with "ICT" throughout the document.
8	DHS	IER Support	E	3	163		For the sake of the Preliminary Framework, are IT and ICS the only two umbrella categories being discussed? **Rationale:** Are other IT systems/assets such as Financial Business Systems binned into IT? There is specific binning just to "IT" and "ICS", but want to ensure organizations understand the context of terms are being captured in the Preliminary Framework.	On page 1, give examples of IT or create a glossary term and/or a footnote (on page 3) that explains which systems/assets are explicitly binned under Information Technology such as Financial, Healthcare, Comms, etc. And what specifically is meant by ICS?
9	DHS	NIC		3	169	1.2	Recommend removing "While not a risk management process itself"	Keep everything after "the Framework uses…"
10	DHS	IER Support	E	3	171	1.2	Make "assessessment" plural to stay within tense	"utilizes risk assessments"
11	DHS	IER Support	T	5	202	2	See comment number 4 above.	
12	DHS	ISS	Administrative	5	207	2.1	Add a definition or example of "Informative Reference" or a pointer to more info below.	

13	DHS	NIC		5	208	2.1	While thie "Framework Core Structure" is not a checklist, it is a "fill in the blank product". This should more closely follow isk analysis since it does not truly list outcomes and why something is being done (even if it is obvious to IT personnel)	Arrange process to place this action where it belongs
14	DHS	Zerbi	Administrative	6	237	footnote	Where is the Compendium? How can a person access it? Is the Informative References column in Appendix A the Compendium?	Please include how to obtain Compendium in the footnote or clarify that Appendix A Infromative References column is the Compendium.
15	DHS	NCCIC Policy		7	242	2.1	It's unclear why the scope here is limited to IT and ICS. Cybersecurity is cross-cutting in nature; in order to effectively implement this framework, application across additional disciplines will need to be addressed.	This recommendation can perhaps be addressed in Section 1.1 (Overview) by mentioning who must be involved in Framework Implementation after describing the implementation tiers. Specifically something to the effect of "though the functions in this framework apply to IT and ICS, they are managed by..." A good example to make the point may be management of insider threats, and the coordination across HR / IT functions required to effectively manage insider threats.
16	DHS	NIC		6	243	2.1	Whose "insitutional understanding" is being developed? If this is a strategic document for use by CEO, CFO, EMs, etc. more common language and themes need to be present	If the goal of this document is to create understanding among decision makers and leaders within an organization with an intention to improve resiliency and mitigation the material requires common language and context so that the CEO impresses upon the workforce why end user security practices are critical.

17	DHS	NCCIC SWO / NCCIC Policy		6	244	2.1	Through this point of the document, there has been no mention of external service providers. In this sentence, for example, “organizational” is used. While it may be intended to encompass external providers, the scope is unclear. It may be worthwhile to include a footnote here that draws attention to risks that may exist through the use of external service providers (Internet access, cloud storage/apps, managed security services providers) so unique considerations are not overlooked by anyone relying on Framework guidance.	Recommend considering the addition of a footnote to mention how risk may be impacted depending on how much (and what parts) of ICT are provided by external providers.
18	DHS	IER Support	T	7	282		Stating the Framework Profile is a "tool" may lead to confusion as both the Current and Target profiles are capability and resource indicators. The Framework profile is a construct to facilitate action. **Rationale: Generally, when the term "tool" is used, we tend to think of a resource that is leveraged to solve a problem or add value.**	Suggest removing "...is a tool..." and reword to "A Framework Profile (“Profile”**) enables** 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."
19	DHS	Odderstol	E	9	330	2.4	Use of "critical infrastructure" does not meet earlier definition.	Suggest changing to "critical assets/resources"
20	DHS	NIC		9	334	2.4	While the statement about risk management occurs within the context of a tier, the front matter of this document states this is not a risk management process	Check document for conflicting ideas and statements
21	DHS	NIC		10	373	2.4	predictive behaviors are often discovered through the use of an appliance. Few organizations have the capability or the knowledge base to conduct predictive analysis, which this statement hints at.	Revise language so that the concepts match the reality of the non-industry ready (i.e. leader without a cyber background)

22	DHS	ISS	Substantive	11	387	2.4	Change from "Organizations should consider leveraging external guidance, such as information that could be obtained from Federal government departments and agencies" to Organizations should consider leveraging external guidance from the Federal government departments and agencies that act as their Sector-Specific Agency (SSA), which guide protective measures for their sector. Information Sharing and Analysis centers can also provide valuable assistance, and organizations can also use existing maturity models, or other sources to assist in determining their desired tier. Note: this will help identify whom organizations can approach for help, reinforces current homeland-security relationships and reinforces federal and private-sector relations as called for in the National Infrastructure Protection Plan.	Change from "Organizations should consider leveraging external guidance, such as information that could be obtained from Federal government departments and agencies" to Organizations should consider leveraging external guidance from the Federal government departments and agencies that act as their Sector-Specific Agency (SSA), which guide protective measures for their sector. Information Sharing and Analysis centers can also provide valuable assistance, and organizations can also use existing maturity models, or other sources to assist in determining their desired tier.
23	DHS	NIC		12	437	3.3	This section is very abstract for those without a cyber background. Additionally, those who will make changes are often not those with a cyber background especially stakeholders	Revise with common language, include graphics that depict flow and relationships

24	DHS	Jones	Administrative	12	445	3.3	Protected Critical Infrastructure Information (PCII) The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances voluntary information sharing between infrastructure owners and operators and the government. PCII protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data. The Department of Homeland Security (DHS) and other Federal, State, tribal, and local analysts use PCII to: Analyze and secure critical infrastructure and protected systems, Identify vulnerabilities and develop risk assessments, and Enhance recovery preparedness measures.	A critical infrastrucutre owner/operator, haiving identified an external partner on whom that infrastructure depends, may use a Target Profile to convey Categories and Subcategories. The exchange of information identifying CI may be secured by using the government's Protected Critical Infrastructure Information (PCII) protocol.
25	DHS	Karolyn Miller (x2322)	G	13	457	Appendix A	It would be beneficial to critical infrastructure sectors that do have regulatory requirements (e.g. Healthcare, Energy) to see the corresponding section of their standard (e.g. HIPAA, NERC) included as Informative Reference in addition to the references to ISO, COBIT, and NIST controls.	Add regulatory references to Framework Core table.

26	DHS	Landesberg	E (We are using "E" to indicate our critical, substantive comments)	28	485	Appendix B	While NIST 800-53 Rev. 4 Appendix J is valuable as an Informative Reference, relying upon it as the *sole* Informative Reference could be confusing, as Appendix J is Privacy Act-focused and applicable to federal departments/agencies and their contractors. Suggest that additional Informative References more closely targeted to the private sector be referenced - at a minimum would add the NSTIC FIPPs	1. Would expressly explain that Appendix J is intended for Feds and their contractors, and that some provisions will not be directly applicable to the private sector, though the general framework, because FIPPs-based, is good guidance. 2. Add the National Strategy for Trusted Identities in Cyberspace (NSTIC) Fair Information Practice Principles (FIPPs) as an Informative Reference (http://www.nist.gov/nstic/NSTIC-FIPPs.pdf)
27	DHS	NPPD Privacy	E	28	485	Appendix B	The methodology well reflects the FIPPs, but there needs to be more explanatory material about how to implement it	A good place to do this would be in an expanded Section C.7. (see Comment 23 below). While certain steps in the methodology would help to protect civil liberties, the methodology does not go far enough substantively regarding civil liberties protections. Defer to DHS CRCL on what that substance should be.
28	DHS	NPPD Privacy	E	28	491	Identify/Asset Management	Organization should not only identify but should also understand that privacy and civil liberties implications of all PII they collect or retain.	REVISE TO READ: Identify and understand the privacy and civil liberties implications of all PII of employees, customers, or other individuals that may be impacted by or connected to cybersecurity procedures, including PII that an organization processes or analyzes, or that may transit the organization's systems, even if the organization does not retain such information.
29	DHS	NPPD Privacy	E	29	491	Identify/Governance	It is important to note that sharing PII must only be for a purpose compatible with the purpose for which the PII was originally collected	Section IV: ADD "originally" between was and collected.

30	DHS	Landesberg	E	28	491	Governance	Add NSTIC Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, and Data Quality and Integrity, and Accountability and Auditing FIPPs as Informative Resources	**NSTIC FIPPS Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII). **Individual Participation:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII. **Purpose Specification:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used. **Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). **Use Limitation:** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected. **Data Quality and Integrity:** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. **Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.
31	DHS	NPPD Privacy	E	29	491	Identify/Risk Assessment	Organizations should have SOPs in place to help them determine the differences between PII and information that could be considered PII and is actually relevant to a known or suspected cyber threat.	Recommend adding an example of a phishing email or other type of cyber threat where PII is used as part of that threat.

32	DHS	NPPD Privacy	E	30	491	Protect/Access Control	It is important to also reduce the collection of PII to the minimum necessary.	ADD: "collection" so that the sentence reads: Limit the collection, use and disclosure of PII....
33	DHS	NPPD Privacy	E	30	491	Protect/Awareness and Training	Recommend including specific role-based awareness and training for cybersecurity analysts or those that handle cyber threat information.	REVISE TO READ: Have regular training for employees and contractors on following such policies and practices, including specific role-based awareness and training for cybersecurity analysts or those that handle cyber threat information.
34	DHS	Landesberg	E	30	491	Data Security	Add the NSTIC Security FIPP	**NSTIC FIPPs Security:** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
35	DHS	NPPD Privacy	E	31	491	Detect/Anomalies and Events	Organizations should have procedures that implement their policies	REVISED TO READ: Have policies and procedures to ensure that any PII that is collected, used, disclosed, or retained is accurate and complete.
36	DHS	NPPD Privacy	E	31	491	Detect/Security Continuous Monitoring	One way to provide transparency is through notice.	REVISE TO READ: Provide transparency into the practices through adequate notice.
37	DHS	NPPD Privacy	E	31	491	Detect/Detection Processes	Recommend adding “civil liberties” and changing “detect” to detection.	REVISE TO READ: Establish a process to coordinate privacy and civil liberties personnel participation in the review of policy compliance and enforcement for detection activities.
38	DHS	NPPD Privacy	E	33	491	Respond/Analysis	If the PII is retained and is necessary to the cyber threat, chances are that it is not accurate or complete.	Deleting second sentence and replacing with the following: If PII must be retained, have policies, which include an oversight and approval process, in place that outline the circumstances in which the PII may be retained.
39	DHS	NPPD Privacy	E	34	491	Respond/Mitigation	One way to provide transparency is through notice.	REVISE TO READ: Provide transparency concerning such methods through adequate notice.

40	DHS	NPPD Privacy	E	35	491	Recover/Communications	Communicating the use or disclosure of PII as part of an incident can be sensitive.	Recommend adding an example.
41	DHS	McNeely	S	29	491		While traditional civil liberties concerns are applicable to only ~10% of CI entities (those that are government owned or operated), individual rights issues may be present in many CI entities and a cybersecurity program involving communications monitoring should make accomodations for observing the legal protections attached to certain sensitive types of communications. We anticipate there may be some stakeholder pushback, but in essence, this expansion of the section merely reminds CI entities to meet their legal obligations with respect to protecting individual rights tied up in communications.	Identify contractual, regulatory and legal, including (where applicable) Constitutional, requirements that cover: i) PII identified under the Assets category; and ii) Any cybersecurity measures that may implicate protected activities or otherwise legally protect individual rights, for example, interception of electronic communications under the Electronic Communications Privacy Act, communications covered by HIPAA, FERPA, or laws protecting specific categories of communications, or other civil liberties and individual rights considerations where applicable.
42	DHS	McNeely	S	30	491		To avoid objections by private sector CI entities to the focus on "civil liberties" suggest changing the phrasing to more inclusive language speaking to legally protected individual rights. This language makes the section much more relevant to the 90% or so of CI entities that are private sector actors.	Senior executive support is critical for building a cybersecurity culture that is respectful of privacy and applicable civil liberties and legal protections of individuals and individual rights.
43	DHS	McNeely	S	33	491		Again, this language is to clarify the scope of the practices to protect individual rights, particularly with respect to private sector CI entities. This does not impose new duties, but is a reminder to check on the legal protections that are applicable and to live up to existing legal obligations protecting the individual.	Respond/Response Planning: For example, when PII is at risk, an organization may need to consider which security activities to perform, whereas when PII is used for response, an organization may need to consider how to minimize the use of PII to protect an individual's privacy or, where applicable, their civil liberties or legally protected individual rights.

44	DHS	McNeely	S	34	491		Again, this language is to clarify the scope of the practices to protect individual rights, particularly with respect to private sector CI entities. This does not impose new duties, but is a reminder to check on the legal protections that are applicable and to live up to existing legal obligations protecting the individual.	Respond/Mitigation: When considering methods of incident containment, assess the impact on individuals' privacy and where applicable their civil liberties or other legally protected individual rights, particularly for containment methods that may involve the closure of public communication or data transmission systems. Provide transparency concerning such methods.
45	DHS	McNeely		34	491		Again, this language is to clarify the scope of the practices to protect individual rights, particularly with respect to private sector CI entities. This does not impose new duties, but is a reminder to check on the legal protections that are applicable and to live up to existing legal obligations protecting the individual.	Respond/Improvements: When considering improvements in responding to incidents involving PII, distinguish whether the incident put PII at risk, whether the organization used PII in responding to the incident, or whether the executed response plan may have otherwise impacted privacy or where applicable civil liberties or other legally protected individual rights.
46	DHS	McNeely	S	35	492		Again, this language is to clarify the scope of the practices to protect individual rights, particularly with respect to private sector CI entities. This does not impose new duties, but is a reminder to check on the legal protections that are applicable and to live up to existing legal obligations protecting the individual.	Recover/Improvements: When considering improvements in recovering from incidents involving PII, distinguish whether the incident put PII at risk, whether the organization used PII in recovering from the incident, or whether the executed recovery plan may have otherwise impacted privacy or where applicable civil liberties or other legally protected individual rights.
47	DHS	NPPD Privacy	E	36	507	Appendix C	Civil Liberties should also be included	ADD: "and Civil Liberties" after the word "Privacy"
48	DHS	NPPD Privacy	E	37	543	C.2	Privacy and civil liberties must be protected during sharing.	ADD: "while protecting the privacy and civil liberties of individuals." after the word "sectors"
49	DHS	NPPD Privacy	E	37	545	C.2	Individuals must also be protected	ADD: "or individuals" after the word "organization"
50	DHS	NPPD Privacy	E	37	547	C.2	PII should be removed.	ADD after the word "to": "identify and delete any personally identifiable information not related to the cyber threat,"

51	DHS	NPPD Privacy	E	37	561	C.2	Privacy and civil liberties consideration should be added	ADD "privacy and civil liberties considerations," after the word "requirements,"
52	DHS	NPPD Privacy	E	38	613	C.7	Civil Liberties should also be included	ADD: "and Civil Liberties" after the word "Privacy"
53	DHS	Jones	Administrative	44	763	Appen. F	Insert definition of PCII	Protected Critical Infrastructure Information (PCII) The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances voluntary information sharing between infrastructure owners and operators and the government. PCII protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data. The Department of Homeland Security (DHS) and other Federal, State, tribal, and local analysts use PCII to: Analyze and secure critical infrastructure and protected systems, Identify vulnerabilities and develop risk assessments, and Enhance recovery preparedness measures.
54	DHS	NIC		2	118, 119	1.1	The concept of the interconnectivity of the five functions (mission areas) should be illustrated early and throughout the document since they are strategic in nature.	Review themes, terms, and language.
55	DHS	Zerbi	Substantive	7	269, 277		How do activities under "Response: Improvements" differ from "Recover: Improvements"?	Please expand on activites for improvements under each category to illustrate the difference or use an alternative word for "improvements".

56	DHS	NCCIC Policy		8	310-317	2.3	The Framework seems to identify a cyclical, tiered, top-down approach to coordinating implementation. Top-down may not always be practical or the most effective means of coordinating implementation. While content provided by different levels of the organization may be inherently hierarchical in nature, the activities may be initiated and/or executed at any level of the organization; it may be neccessary to reach across different levels throughout the process.	Recommend mentioning that bi-directional communication will be necessary throughout implementation, that a feedback loop is critical, and that activities may be triggered at any level of the organization, particularly given the potential for different elements of the cycle (i.e. individual profile development v. overall priorities development) to have a very different shelf life.
57	DHS	Odderstol	E	12	426/427	3.2	Need clarity around "gaps" and how an organization would assess them.	Suggest re-wording to address current v. needed capabilities discovered after conducting a risk assessment. Then addressing the gaps between capabilities within a risk management strategy.
58	DHS	Odderstol	E	12	439/446	3	as with comment 7 above	
59	DHS	Zerbi	Administrative	13	462-463	Appendix A	This part of the sentence is repetitive with line 460-461: "and additional Categories, Subcategories, and Informative 462 References may be added to the Profile."	Delete

							We are concerned that this section is both inaccurate and unnecessarily defeatist regarding the existence and usefulness of applicable guidelines for protecting privacy. Contrary to the current language, Fair Information Practice Principles, which are reflected in many federal and private-sector privacy regimes, most recently in the National Strategy for Trusted Identities in Cyberspace, provide precisely the “standardized guidance” the draft states is lacking. They are a well-settled and effective framework for protecting against and mitigating privacy risks. The draft states that “there are few identifiable standards or best practices” addressing how to mitigate potential harm to individuals from cybersecurity activities, yet the FIPPs do just that, in a manner that allows the flexibility to adapt the guidance to individual business needs. While it is true, as the draft states, that organizational policies often focus more on business risks than on the risk of harm to individuals, the FIPPs are intended precisely to provide guidance on minimizing harm to individuals. In short, rather than disparaging and mischaracterizing the FIPPs, the draft should be supportive of their implementation. It should expressly encourage participants to implement the FIPPs, and it should explain how to use the Methodology in Appendix B and how the steps taken there can be integrated into the other activities championed by the Framework.	Replace current language with the following: Appropriate Privacy and Civil Liberties protections should be embedded at the beginning of all data collection, system development, and information sharing activities and any information sharing should be in accordance with applicable confidentiality statutes, both state and federal. Organizations should be transparent about information collection and sharing activities, and ensure that information is maintained and used only in accordance with government and private sector authorities. Privacy and civil liberties offices should be included early in the development and review process to ensure privacy and civil liberties risks are identified and mitigated appropriately. To protect privacy, organizations should consider executing a Privacy Threshold Analysis (PTA) or similar assessment to determine if personally identifiable information (PII) will be collected, maintained and/or shared. If PII will be collected and/or shared, then programs should consider conducting a Privacy Impact Assessment (PIA). Executing a PIA, which analyzes in greater depth how PII is collected, stored, protected, shared, and managed, is a best practice that should be considered by all stakeholders. Privacy requirements involving the collection, use,

60	DHS	NPPD Privacy	E	38-39	614-632	C.7	It is important not to conflate privacy protections with civil liberties protections. While implementing the FIPPs may further civil liberties protections, doing so does not fully address civil liberties concerns. The FIPPs are privacy-focused guidance. We defer to our colleagues in DHS CRCL on language they submit concerning how to implement civil liberties protections.	
61	DHS	Jones	Administrative	1	footnote	1	Footnote #2: delte KR from CIKR. KR isn't used anymore.	
62	DHS	Susan Sheely ((480) 403-3336)	E	6	footnote 3		Grammar edit	Change the word "includes" to "including", or change to "and includes"
63	DHS	Pomerleau	Administrative	na	na	na	Include information with POCs and hyperlinks where folks can get technical advice and remain current on updates to practice, guidelines, etc. this is a dynamic and rapidly changing field of technical issues	
64	DHS	Pomerleau	Administrative	na	na	na	Document is unclear on the privacy and security aspect of how the framework provides useful information to users or the IT specialists at a company or elswewhere	
65	DHS	NCCIC SWO		18	NA	Appendix A	DATA SECURITY – This seems like a non-standard way to express data state. Usually described as rest, transit and process.	It may be of use to modify or acknowledge the variance to ensure terminology resonates among technical SMEs.
66	DHS	NCCIC SWO / NCCIC Policy		22	NA	Appendix A	What is DLS? Recommend defining all acronyms at first use.	Recommend defining DLS.

67	DHS	NCCIC SWO / NCCIC Policy		28	NA	Appendix B	GOVERNANCE – It may be of use to mention the importance of identifying international PII laws/rules that may apply to data or customers/suppliers. Organizations may also need to consider PII rules that apply to data shared by partners (when those rules are more stringent than organization's own policies) and to ensure that external services providers adhere to the organization's same data handling PII rules when they have access to the organization's data.	Recommend incorporating relevant language within this subcategory.
68	DHS	Landesberg	G				The Framework should even more strongly emphasize implementation of Fair Information Practice Principles (FIPPs) as the basis for protecting privacy. Our comments below are intended to bolster the EO 13636 requirement that privacy be protected consistent with the FIPPs. We defer to DHS CRCL for their input on language strengthening CRCL protections, to the extent relevant in this private-sector focused Framework.	Please reconsider comments previously submitted as well as comments on Appendix B below. With respect to Appendix B, at a minimum, add private-sector-based versions of the FIPPs to the list of Informative References in Appendix B.
69	DHS	M. Sawyer	G	15-16		Risk Assessment	The 5 steps (ID.RA-1 through ID.RA-5) are not clear; asset vulnerabilities are idntified in a step before vulnerability infomration is received, there is no explicit analysis function, risk is not assessed before responses are identified.	Modify the subcatagories: One suggestion: RA-1 - Vulnerability information is received; RA-2 -Vulnerability information is anakyzed and asset vulnerabilities are identified and documentd; RA-3 - Threat information is received; RA-4 - Threat information is analyzed to identify and document threats to assets; RA-5 - use current RA-4; RA-6 - Risk to assets are assessed and documented; RA-7 - Risk responses are identified and documented

70	DHS	M. Sawyer	G	22		Detect	The use of intelligence or contexual information regarding threats is understated.	DE.AE-3 Contextual threat data is correlated with event data to determine full extent of event and to identify potential related events that may have already occurred and need to be identified or may occur in the future
71	DHS	T. Leaf	G	13-15		Table 1	Table 1 appears to chart a linear process for assessing & mitigating risk. Although mentioned in section 2.4, Framework Implementation Tiers, it may be useful to emphasize the need for the RA to evolve with the AM & BE.	As the AM & BE evolve, the RA is continuously updated to reflect the most current state of risk to the enterprise.
72	DHS	McNeely	S	34			Again, this language is to clarify the scope of the practices to protect individual rights, particularly with respect to private sector CI entities. This does not impose new duties, but is a reminder to check on the legal protections that are applicable and to live up to existing legal obligations protecting the individual.	Recover/Recovery Planning: ...For example, when PII is at risk, an organization may need to consider which security activities to perform, whereas when PII is used for recovery, an organization may need to consider how to minimize the use of PII to protect an individual's privacy or where applicable civil liberties or other legally protected individual rights.

