#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	BAE Systems Applied Intelligence	Miriam Howe	G			Appendix A and section 2.4	The Framework doesn't appear to address how to measure the effectiveness or strength of the controls specified in the Subcategories. The only measures provided are for risk management, program integration and external interaction (Section 2.4). This may create a challenge when trying to compare profiles (e.g. target and current, or between organizations within a sector).	Addition of measures of effectiveness for each of the Subcategories included in the core Framework. Scales depicting such measures are pictured in section 2.2, Figure 2, but the necessary criteria are not defined. Measures of effectiveness need to be proportionate to the size and type of an organization implementing the Framework. Therefore the criteria for measurement will likely need to be multi-dimensional to account for these variables.
2	BAE Systems Applied Intelligence	Miriam Howe	E	8-9		2.3	Priorities and exposure will change over time, particularly if improvements are made that allow focus to be relaxed in one area and concentrated in another. This is well represented in the diagram in 2.3. However, the Framework provides no suggestions for the frequency that decisions and priorities should be reviewed.	The Framework should prompt for regular review of objectives and priorities. This could be achieved by suggesting that the duration (or time bounds) of each objective and priority should be identified at the time of agreement.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
3	BAE Systems Applied Intelligence	Dan Carr	G	1	91-93	1	The claim that 'the use of standards will enable economies of scale to drive innovation…' is a little bit abstract, there should be some evidence that supports this claim. Cost effectiveness is not addressed anywhere else in the document.	This claim should be supported by examples to make this argument more robust. To more broadly address cost effectiveness of the Framework we need to consider how testing and demonstration of cost effectiveness can be achieved. This is not a simple thing to do as an organization requires a solid understanding of their risk posture in order to measure cost effectiveness of any new security controls. Additional thought is needed to include guidance for setting Key Performance Indicators (KPIs) for cost effectiveness as part of the Framework.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
4	BAE Systems Applied Intelligence	Dan Carr	G				The Framework provides a common language and mechanism for organizations to assess their security posture and their target posture, and how they can measure some of the improvements. However, it provides little assistance for how organizations are actually supposed to approach and invest in this process of improvement – a common problem for many, i.e. where and how do they start? There is limited guidance for how to structure the approach and how to identify which areas of the Framework to prioritize and for what reasons. These issues need to be considered for organizations at varying levels of security maturity, for example if a company has already invested in cybersecurity risk assessment, subsequently re-doing that assessment in the context of the Framework would be costly and disruptive. There is no mention of alternative 'entry points' for organizations that are not starting from scratch.	The measures of effectiveness outlined in the suggestion for comment 1 would aid this, helping organizations to better align themselves with the Framework, particularly those that are more mature. The Framework should offer some guidance on how to prioritize Subcategories through cost benefit analysis. A series of case studies that demonstrate how organizations could go about implementation of the Framework would be a valuable addition. These case studies should span the varying example organizations, both in terms of size, security maturity and CI sector. Case studies should include an example of a business that has already done some risk management through a separate framework and an example through the lens of a small business.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
5	BAE Systems Applied Intelligence	Dan Carr	G				The Categories (without specified measures of effectiveness for each - see comment 1), combined with the measurement of each organization's current profile, are likely to encourage organizations to aim for implementing the highest 'bar' in every category in order to be perceived as 'good', especially where the Framework is being used by suppliers to meet customer's requirements. The danger here is it becomes more of a marketing tool rather than an effective portrayal of an organization's risk posture and could lead to wasted resources in addressing categories that are largely irrelevant for that organization. This could lead to reduced cost effectiveness.	The addition of measures of effectiveness outlined in suggestions for comment 1 would aid this point. To help prevent the Framework being used as a marketing tool by suppliers to CI organizations, customer organizations will need a process for reviewing a supplier's measures of effectiveness as part of supply chain assurance. Also include an additional case study (to those described in comment 4) that focuses on cost effectiveness and demonstrates that you don't have to achieve full marks in all categories.
6	BAE Systems Applied Intelligence	Dan Carr	G	39		C.8	As identified in areas for improvement, the supply chain is an ever growing concern for CI. The process of ensuring supplier compliance will be costly and challenging and may actually shrink the size of the accessible market.	This area for improvement should be addressed as a priority and guidance should be provided on how companies implementing the Framework can mandate or request aspects of the Framework of their suppliers.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
7	BAE Systems Applied Intelligence	Dan Carr	G				There will be many smaller companies that form part of the wider CI ecosystem that will ultimately have to comply with the Framework in order to meet supply chain assurance requirements of the larger companies as well as their own risk management objectives. The Framework as its stands does not seem appropriate for them because of the resources required to implement, which smaller firms are less likely to have available.	The Framework needs to address how smaller organizations can adapt the Framework to be relevant to them. This could be done through case studies, as suggested for comment 4, that demonstrate how the Framework could be implemented for organizations of varying size.
8	BAE Systems Applied Intelligence	Harriet Griffiths	G	1	90-91	1	It is stated that the Framework will evolve, however no further detail is provided for how that will work in practice, for example how often new versions are likely to be released, the mechanism for release or the criteria that will prompt a new release. This is important to set expectations for how often the guidelines are likely to change.	Include a section on document management that details when the Framework will be updated, the criteria that will prompt a new release and the process for publishing new releases.
9	BAE Systems Applied Intelligence	Harriet Griffiths	G	12		3.4	There is only minimal information on how users of the Framework will be able to contribute ongoing suggestions as they start to implement the Framework and come across useful approaches. Section 3.4 indicates that this kind of evolution is likely to happen, particularly for Subcategories with limited current guidance. However, no information is provided on how new material can be contributed and incorporated into future iterations of the framework. This is important to continue the involvement from industry in the evolution of the Framework.	Consider hosting a wiki or other collaborative application that organizations can use to share approaches (e.g. additional standards) for implementing each part of the Framework. This would serve to provide up to date information for other users of the Framework and would be able to inform new iterations of the Framework document.

#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
10	BAE Systems Applied Intelligence	Miriam Howe	G	15-16		Appendix A - Identify - RA	The Framework includes controls for gathering and documenting threat information under the Identify function. However there is no guidance provided on how to actually use that threat information to enhance detection capabilities. As threat information sharing increases through multiple initiatives (ISACs, Infragard, ECS etc.) the volume of threat information will increase and it is important for organizations to be able to manage and effectively use threat information. This is alluded to in the suggested improvement in section C.2.	Provide additional detail, either in Identify or Detect on: - How threat information should be disseminated and who it should be sent to. - How threat information should be organized, contextualized and prioritized in terms of its relevancy to the organization. - How to translate threat information into indicators that can be used for threat detection.