#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	ReliabilityFirst	David Sopata	G, T	PDF 9, document 6	245	2.1	: It is not clear whether Asset Management within the Identity function includes Configuration Management and/or Baselines. In addition to ensuring that an inventory list is up-to-date, Asset Management should include Configuration Management and/or Baselines. Configuration Management and/or Baselines address configurable attributes that tie to an Asset or a set of Assets. Identifying the establishment of Baselines is important for detection of anomalies and changes within a system.	The Identify Function includes the following categories of outcomes: Asset Management, Configuration and Security Baselines, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.
2	ReliabilityFirst	David Sopata	G, T	PDF 10 document 7	261	2.1	The Detect function should fully address baselines. Within the detect function, understanding and establishing baselines for assets and for network traffic are crucial concepts that should exist throughout the framework. Without baselines, it is impossible to detect anomalies. In addition, this seems to be somewhat addressed in the Anomalies and Events category under DE.AE-1. The Anomalies and Events category only identifies baselines of normal operations and procedures, not the assets or network traffic itself.	Configuration and security baselines defined within the Identity function are the foundation that enable entities to determine that there has been a change or an event within their environment.

3	ReliabilityFirst	David Sopata	G	PDF 10 document 7	292	2.2	It seems that creating a Target Profile can pose difficulties when a critical infrastructure operator/owner is starting from the beginning and has no real frame of reference. Perhaps tiers based on the entities' inherent risk based on size and/or potential impact to the rest of their environment and to the rest of the US would be helpful in assisting new participants in target profiles. Is there any future concept of critical infrastructure operator/owner anonymously reporting their internal current/target profiles as a national dashboard by critical infrastructure type? Without some type of accountability, management may disregard internal findings and opt for an inappropriately low Target Profile. Will this be tied to the Cybersecurity Awareness Act of 2013?	
4	ReliabilityFirst	David Sopata	G	PDF 11 document 8	310	2.3	It seems that someone at the senior executive level can easily communicate mission priorities and available resources. However, it may be difficult for them to communicate overall risk tolerance to the business/process level. As related to the 3rd set of comments, past experience indicates that many senior executives may not be aware of high-level risk that can happen at the business/process level to communicate an overall risk tolerance. Is this meant to be a way for management to "put a stake in the ground" and then revisit it over time with Operations?	

5	ReliabilityFirst	David Sopata	G,T	PDF 14 document 11	412	3.2	Within the steps of creating a new cybersecurity program, please refer back to the first comment regarding the importance of assessing and establishing configuration baselines for assets. I believe that configuration baselines are an integral component of asset management. It should be identified whether configuration baselines exist or not.	Step 1: Identify. The organization identifies its mission objectives, configuration baselines of related systems and assets, regulatory requirements and overall risk approach.
6	ReliabilityFirst	David Sopata	G,T	PDF 15 document 12	441	3.2	The bullet "An organization may utilize a Target Profile to express requirements to an external service provider (e.g., a cloud provider) to which it is exporting data." seems to further burden the service providers with another security framework on top of the many frameworks/regulations that they have to comply with such as: FISMA, HIPAA, FedRAMP, FERPA, etc. The framework has provided some cross-reference within this model, but it may be helpful to provide additional guidance on managing service providers and using the Compendium to help service providers effectively communicate their security posture to their customers who require them to adhere to these broad and numerous regulation/security frameworks.	

6	ReliabilityFirst	David Sopata	T	PDF 16 document 13	466	Appendix A: Framework Core	Similar to the first comment, the Asset Management Category within the Identify Function should contain a subcategory of identifying and/or assessing configuration baselines for physical devices, systems, software platforms, and/or applications. Configuration Management and/or Baselines address configurable attributes that tie to an Asset or a set of Assets. Identifying the establishment of Baselines is important for detection of anomalies and changes within a system.	Add an ID.AM-7: Identify and assess current configuration baselines for assets such as physical devices, systems, software platforms (such as databases, applicantion services), and/or applications.