#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Idaho National Laboratory	Rita Wells	G	all			If the intent is to work with asset owners and operators of critical infrastructure, use protection instead of target. Targets are attacked while assets are protected. Otherwise sounds like the Military wrote the framework.	Change 'Target' profile to 'Protection' profile
2	Idaho National Laboratory	Rita Wells	T		74		Threat information sharing is required (Sections 1.2 Likelihood of risk event, and 2.1 assessing threats). The U.S. Government does not have a good track record on sharing threat information with asset owners and operators. The problems are many. A) Normally dissemination of adversaries and their capabilities in threat characterization requires security clearances rarely found in industry. B) If temporary clearances are granted to asset owners and operators for information sharing rarely is that information more than what is available open source. C) If open source critical infrastructure threat providers are used, the threat does not correlate to asset owner architectures (which would create actionable information sharing) - this is the same problem USG has in communicating with industry. Focusing on code and not the adversary can provide value to the asset owner. Capabilities of the exploit, potentially exploitable newly discovered vulnerabilities or techniques used for either can be tied to asset owner architectures or components creating more actionable threat information.	Focus on emerging exploits, vulnerability discovery and new attack techniques with impact to asset owner architectures.
3	Idaho National Laboratory	Rita Wells	T	1		Section 1.0	No evidence that process laid out will be repeatable, timely enough to match the dynamic nature of the cyber threats.	Feedback to process improvement is missing. Addressing cyclical nature of ongoing process would address issue.

4	Idaho National Laboratory	Rita Wells	T	8	315	Section 2.3	The impact assessment is to inform senior executive level - implies senior level does not understand risk when dealt with daily. If this is truly a repeatable continual process, the impact could be understood in the process improvement to increase the reliability or up time of the system against cyber threat. Allowing for continual process improvement is a value-add for industry.	Focus on the ability to use the impact assessment for continual process improvement.
5	Idaho National Laboratory	Rita Wells	T	11	397	Section 3.1	Implementation on high level functions will vary greatly between IT systems and different ICS configurations. Ensure the implementation is not forced to be rank order sequential. For example, protecting data in transit may be more feasible than protecting data at rest on mid to end devices in an ICS configuration. Asset management is more likely on a static small process control system than a large geographically distributed ICS, but patching vulnerabilities may be more problematic on the process control environment.	Implementation needs to be tailored to architecture and not forced step sequential layers to accommodate ICS.
6	Idaho National Laboratory	Rita Wells	T	3	177	Section 1.1	Including the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) would be valuable.	Including the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) would be valuable.
7	Idaho National Laboratory	Rita Wells	T	6	242	Section 2.1	Apply to both IT and ICS – at different levels and between ICS configurations to different levels as well.	Apply to both IT and ICS – at different levels and between ICS configurations to different levels as well.
8	Idaho National Laboratory	Rita Wells	T	7	294-296	Section 2.2	Gaps between the Current profile and the Target profile allows for creation of prioritized roadmap….is too government based. The goal for industry is to focus limited cyber protection resources to the most likely exploitable components and configurations that could impact the most critical assets.	Remove roadmap, industry doesn't need roadmaps.

9	Idaho National Laboratory	Rita Wells	T	11	386-389	Section 2.4	The desired tier will be based on feasibility to implement protections. The threat analysis will fall mainly on the industry processes since they understand the impact to their systems better than anyone and information sharing centers are getting better but do not correlate to asset owner configurations.	Refocus section to acknowledge that industry has the greatest understanding of impact to their systems from any threat.
10	Idaho National Laboratory	Rita Wells	T	11	418-420	Section 3.2	…discern the likelihood of a cybersecurity event...probability of the adversary attacking is difficult to share with industry due to lack of classified threat intelligence.	Refocus this section on the capabilities of the exploit or vulnerability on asset owner's configurations will provide probability factors without the problematic classified information sharing.
11	Idaho National Laboratory	Rita Wells	T	12	451	Section 3.4	Adding other informative references such as the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) would be valuable.	Adding other informative references such as the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) would be valuable.
12	Idaho National Laboratory	Rita Wells	G	13		Appendix A	Identifying the potential problematic areas for ICS would be beneficial for industry to accept. For example ID-AM-3 organizational communications mapped…is more challenging when moving between the corporate and operational environment.	
13	Idaho National Laboratory	Rita Wells	T	16		Appendix A	ID-RA-3 Threats to assets are difficult for tailored configurations in critical infrastructure. If industry waits for the USG to inform them of threats, critical infrastructure will not be protected.	Refocus this need for industry to understand the parts of threats such as impact to exploits and vulnerabilities.
14	Idaho National Laboratory	Rita Wells	T	16		Appendix A	ID-RM-2 Organization risk tolerance is determined and clearly expressed…this is difficult to do with the dynamic nature of cyber threat.	Refocus need for continual cyber protection process improvement.
15	Idaho National Laboratory	Rita Wells	T	16		Appendix A	PR.AC-1 Identities and credentials managed for authorized devices and users is rare for mid and end devices in ICS and PR.AC-2 physical access secure is rare for geographically dispersed assets.	
16	Idaho National Laboratory	Rita Wells	T	17		Appendix A	PR.AC-3 3rd party stakeholders understand roles - rare agreements for contractual access in ICS exist	
17	Idaho National Laboratory	Rita Wells	T	18		Appendix A	PR.DS-1 Data at rest is protected is rare for mid and end devices in ICS	

18	Idaho National Laboratory	Rita Wells	T	19		Appendix A	PR.DS-5 Protection against data leaks is rare in ICS	
19	Idaho National Laboratory	Rita Wells	T	19		Appendix A	PR.DS-7 Unneccessary assets are eliminated is rare in ICS since vendors allow for asset owers and operators maximum flexibility and default enabled processes to allow ease of installation	
20	Idaho National Laboratory	Rita Wells	T	20		Appendix A	PR.IP-3 Configuration change control processes are in place is rare due to embedded code and commodity of component end devices	
21	Idaho National Laboratory	Rita Wells	T	20		Appendix A	PR.IP-9 response plans are very well exercised in more critical infrastructure but rarely include cyber.	
22	Idaho National Laboratory	Rita Wells	T	21		Appendix A	PR.PT-1 audit logs are very heterogenious in the ICS configurations	
23	Idaho National Laboratory	Rita Wells	T	21		Appendix A	PR.PT-3 Geographically dispurse assets in ICS are common	
24	Idaho National Laboratory	Rita Wells	T	21		Appendix A	PR.PT-4 key management issues with the multiple mid and end devices in ICS is problematic	
25	Idaho National Laboratory	Rita Wells	T	22		Appendix A	DE.AE-3 correlated cyber data is almost non-existent in ICS	
26	Idaho National Laboratory	Rita Wells	T	22		Appendix A	DE.CM-2 physical environment monitored is difficult in the geographically dispurse ICS	
27	Idaho National Laboratory	Rita Wells	T	22		Appendix A	DE.CM-4 Malicious code detected is rare on tailored ICS configurations	
28	Idaho National Laboratory	Rita Wells	T	24		Appendix A	RS.AN-3 Forensics are prefomed - limited forensics capabilities in ICS	
29	Idaho National Laboratory	Rita Wells	T	25		Appendix A	RS.MI-2 incidents are eradicated is problematic to prove a negative 'the malware is gone'	
30	Idaho National Laboratory	Rita Wells	T	28		Appendix B	Privacy and Civil liberties have limited applications in ICS - exception being billing systems connected to ICS or identification numbers for communication services	
31	Idaho National Laboratory	Marlene Ladendorff	T	36	501-508	Appendix C	Portable Devices and Media are a significant concern in ICS operations: hand-held calibration equipment, thumb drives, external hard drives, laptops and tablets	Add portable devices and media to the bulleted list on page 36

32	Idaho National Laboratory	Bri Rolston	G				For the ICS world, there is a need for processes that address risk factors to include threat in an unclassified and useable environment. Linking those risk characteristics to asset owner and operator configurations is another detailed and time consuming process. This CIP Framework is high level and does not address the need to develop these to make the risk analysis useful in an operational setting.	