Comments template for Preliminary
Cybersecurity Framework

Submitted by: ________________________
Date: ________________________

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	2BSecure LLC	Robert Bigman	G/T	All	All	All	The proposed "Framework Core" is supposed to be a set of standards. However, standards are something you can easier measure as **yes** or **no**. How does one measure your proposed standard number PR.DS-1: Data at Rest is protected? If every entity interprets that requirement their own way, it is not a standard but simply a vague notion!	To improve critical infrastructure, this document needs to provide specific/detailed standards for protecting systems, networks, and applications. Simply listing good notions (e.g., PR.DS-1: Data-at-rest is protected), is too broad and subjective. Now, changing that same function to say: PR.DS-1: Data-at-rest on Internet accessible systems is protected via network isolation and encryption actually provides a measurable standard!
2	2BSecure LLC	Robert Bigman	G/T	All	All	All	In line with above comment, I thought one of the goals of the framework was to reach agreement between all public and private organizations, at least, on a minumim set of controls that all organizations will implement. This seems to be missing.	To improve critical infrastructure, this document needs a section that clearly proposes a set of minumim protection controls that all members of the critical infrastructure will provide. For example: "All critical infrastructure SCADA devices will be physcially isolated from Internet access."
3	2BSecure LLC	Robert Bigman	T	16	All	Appendix A. Framework Core	The "Protect" section of the Framework Core is particularly weak. Needs to address numerous critical areas	Need to add requirements for: 1) Malware Prevention (not just detection); 2) O/S integrity mechanisms; 3) Use of logical (or physical) network segregation; 4) Privileged admin. access controls; 5) Use of system hardening standards; 6)Use of encryption as an access control measure.
4	2BSecure LLC	Robert Bigman	G	7	281	2.2	Why have an organization define their current profile BEFORE the target profile? Wouldn't it make more sense to have an organization first develop a profile based on where they want to be and then determine what they need to do based on their existing risk measures.	Recommend organizations first develop a Target Profile, then a current profile.

Type: E - Editorial, G - General T - Technical

5	2BSecure LLC	Robert Bigman	G	9	321	2.4	If is not clear to me what the purpose of the entire "Framework Implmenentation Tiers" is for. Why does an organization need to determine the desired tier? Frankly, one can just as effectively use the framework core without considering their target tier. This does not seem to add value, but I'm not sure what NIST is trying to accomplish.	Suggest this entire discussion/section be removed.
6	2BSecure LLC	Robert Bigman	T	14	ID.BE-1/2		ID.BE-1 and ID.BE-2 need to be rewritten or reworked. I have no idea what the point of either are and how it relates to cyber security. Identifying and communicating things are highly subjective and, again, it is unclear what this does to enhance cyber security.	If there is a cyber security point to be made here, it needs to be better described.
7	2BSecure LLC	Robert Bigman	G	15	ID.GV		The Goverance section is also a little weak and misses some key areas.	Recommend that this section includes: 1) Recommending that every organization have critical cyber security policies in-place. I suggest they use, at a minimum, the SANS key policy templates. Also, need a requirement that measures the degree to which the cyber security program is involved in both tactical IT decisions (e.g., engineering review boards) and strategic IT planning.
8	2BSecure LLC	Robert Bigman	T	16	PR.AC		There should be a requirement in Access Control for organizations to have a central directory service system to enforce access controls to sensitive data.	Add a requirement for a central directory service (e.g., AD) for enforcing access control.
9	2BSecure LLC	Robert Bigman	G	19	PR.DS-7		Not sure what point is being made about "unnecessary assets."	Not a cyber security relevant topic. I suggest you drop it.
10	2BSecure LLC	Robert Bigman	G	20	PR.IP-7		Absolutely to vague to add value and be measured.	Recommend you state specifically what actions constitute "continuously improving protection."

11	2BSecure LLC	Robert Bigman	G	19	PR-IP		One of the biggest concerns with all organizations is controlling users with administrative privileges. However, the proposed standards do not address this concern.	I suggest you add a standard to measure how well an organization "compartments" levels and types of admin. privileges across networks, systems and applications so no single individual can access excessive amounts of information.
12	2BSecure LLC	Robert Bigman	G	21	PR.MA		The maintenance section is missing some key measures.	I suggest you add requirements for: 1) Ensuring that maintenace personnel are appropriately approved/cleared; 2) Media is properly sanitized.
13	2BSecure LLC	Robert Bigman	G	21	PR.PT-1		Well, what if they have a bad audit retentiuon policy or no policy at all. Standards should never assume existence of a policy.	I suggest you first recommend that they actually have an audit policy before you ask if there is compliance.
14	2BSecure LLC	Robert Bigman	T	22	DE.AE		This section seems to have missed stating a recommended standard for both detecting and preventing events.	I suggest that this section include a requirement to have organizations have a program to electroncially detect, analyze and respond to events.
15	2BSecure LLC	Robert Bigman	G	22	DE.CM-2		How can one monitor physical activity to identify cybersecurity events?	Please be clearer regarding what is meant or remove.
16	2BSecure LLC	Robert Bigman	T	23	DE.CM-5		This issue is really unauthorized code, regardless of whether it is mobile across various platforms.	Change to "Unauthorized code is detected."
17	2BSecure LLC	Robert Bigman	T	23	DE		I think you need to make a special mention of detecting zero-day malware, especially rootkits.	I suggest you add a standard here (or in the protection section) that addresses the requirement to detect (and/or) prevent malware for which there is no known signature. This can be accomplished via system/network architecture, monitoring memory processes and/or using processing isolation technology like Bromium.

18	2BSecure LLC	Robert Bigman	T	36	Appendix C		It seems to me that Appendix C is missing a BIG area for improvement, specifically specifying standard for building secure operating systems and coding secure applications.	I suggest you add a topic to Apperndix C that specifies a recommendation for vendors, academia and related IT organizations to work together to develop new standards for how to build secure operating systems and establish coding requirements within languages to ensure they have fewer opportunities for vulnerabilities.