Comment Template for: Draft Profile of Responsible Use of Positioning, Navigation, and Timing

Please submit responses to: pnt-eo@list.nist.gov by November 23, 2020

Special note from reviewer: There is a general need to differentiate PNT systems from cyber systems such as computer and communications systems. As indicated in my comments, it is crucial for understanding PNT security to understand that PNT fundamentally requires protection of signals in a way that does not exist in cyber systems. This needs to be made clear at many steps of the process. This document requires major changes throughout to support this. The document is excellent in terms of cyber data issues, which are critical also to PNT, but PNT has totally different issues, and the PNT Profiles

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
1	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com	ii	94	Abstract	This is unclear: "The PNT serves as the … "	Do you mean "This PNT profile serves as the …", or something else?	Editorial
2	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		305		A fundamental issue that should be highlighted should be added to this bulleted list: "* General prinicples about how PNT systems work"	Add the bullet: "* General prinicples about how PNT systems work"	Technical
3	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		316		The fundamental difference between PNT systems and Cyber systems should be emphasized at the very beginning, so users can understand their requirements.	Add major section before existing "3.1 Risk Management Overview," Such as "3.1 Fundamental principles of PNT" PNT systems differ from data-based systems in that they are dependant on the integrity signals and their timing. Navigation and positioning are generally performed by measuring the time of arrival of a signal and to use the delay from the source transmission to determine current position. Hence, any delay in this signal can change the computed position. This is fundamentally different than data in computer and communications systems, where data are routinely stored and forwarded for processing later. This fundamental difference explains why PNT systems need different care from cyber-	Technical

4	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		394		The example in figure 2 is specific to cyber-systems. For PNT, one should add "signals" as a specific consideration for inventory, as well as add PNT processors separate from software platforms. For example, a physical time-stamping system at the ingress or egress of data in a signal needs special care that no delays are tampered with. This is closer to a software platform (ID.AM-2) than a physical device (ID.AM-1), but is substantially different than software.	"**ID.AM-1:** Physical Devices, signals, and systems …" "**ID.AM-2**: Software platforms, PNT processors, and …"	
5	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		437		Table-2 needs a separate column for PNT signal channels	The column to the left of "Identify appropriate PNT Sources" should be "Identify PNT signal channels"	
6	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		457		Table-3 should follow the same principles as above, emphasizing issues around signals, immediacy, and timing, issues that are substantially different for PNT than exist for data processing machines.		
7	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		464		Table-4 refers to PNT data resilience requirements. The core issue for PNT is signal and time-stamping integrity first. Once there are good time-stamps, PNT systems become like cyber systems, i.e. data processing systems.		
8	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		485		Table-6, again, fails to emphasize signals instead of data.	The phrase "and the system distributing PNT data." should say "and the system distributing PNT signals, time-stamping those signals and PNT data."	
9	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		504		Table-8 similarly, should mention signal transport systems.	"Enable approved access lists for all controls that follow, NTP and PTP time servers, and other PNT systems." should say "Enable approved access lists for all controls that follow NTP and PTP time servers, time signal channels, and other PNT systems."	

10	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		518		Table-10 is titled "Protect Data Security." This is, of course, a critical factor. But there should be a similar list for "Protect PNT Signal Security."		
11	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		541		Table-13 discusses "Protect Protective Technology." There needs to be a section on testing for changes in timing delays as part of this protection. One could loop back a timing signal and continuously monitor the total delay, have multiple differently routed timing methods, etc. Such things are mentioned in passing, but they need to be emphasized.		
12	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		558		Table-15 discusses "Detect Security Continuous Monitoring". Redundancy should be emphasized. This is a fundamental safety principle used throughout industry and technology. In many safety-critical systems, such as fly-by-wire and hydraulic systems in aircraft, some parts of the control system may be triplicated which is formally termed triple modular redundancy (TMR). An error in one component may then be out-voted by the other two. In a triply redundant system, the system has three sub-components, all three of which must fail before the system fails. Since each one rarely fails, and the sub components are expected to fail independently, the probability of all three failing is calculated to be extraordinarily small; often outweighed by other risk factors, such as human error. Redundancy may also be known by the terms "majority voting systems" or "voting logic". See, for example: Redundancy Management Technique		

13	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		574		"Table 17-Response Planning Subcategory Applicable to PNT" should emphasize the need for alternate PNT sources in order to have a fall-over capability. Or at the very least to sever or stop PNT data to prevent false information from being transferred. There should also be a method to communicate status to downstream devices.		
14	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		596		Table 20-Mitigation Subcategories Applicable to PNT appropriately discusses potential transition to alternate PNT devices, but these need to be set up, tested and enabled in advance of any event. Hence it is critical to discuss PNT signals and resilience as mentioned previously.		
15	Marc Weiss Consulting	Marc Weiss, marcweissconsulting@gmail.com		1114		add a definition of "signal"	An example: An electrical impulse or sequence of impulses communicating a specific time to a required accuracy. Can be an electromagnetic signal, or can be a data message with a pre-defined sequence.	