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

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

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
	NextNav				All	Recommend adding some specificity to perhaps provide some examples from different sectors or create a sector specific SSA	Provide some examples from different sectors or create a sector specific SSA	General
	NextNav		14	457	4.1.1	List of technologies can become more comprehensive in this paragraph: "PNT system components may include GPS/GNSS receivers, radio navigation or timing antennas, network switches, IoT/SCADA devices, and NTP and PTP servers."	Proposed text as follows: "PNT system components may include GPS/GNSS and/or other PNT receivers, such as based on terrestrial beacons, radio navigation or timing antennas, network switches, IoT/SCADA devices, and NTP and PTP servers.	General
	NextNav		33	518	4.2.3	Under table column on References (PNT-Specific), add reference to ICD of other PNT systems	Add reference to [MBS ICD] e.g. to DS-1, DS-2, DS-6; see other related comments in this spreadsheet, including comment on suggested addition to Reference section.	General
	NextNav		34	518	4.2.3	Under DS-2, add further content on exploitation of authentication and encryption features of PNT systems	Under subcategory DS-2, add the following content to the second column Applicability to PNT: "Leverage PNT systems that employ authentication and encryption of PNT data as a desirable system feature to protect against data and measurement spoofing attacks."	Technical
	NextNav		35	518	4.2.3	Under DS-6, add further content to recommend use of PNT receivers that implement data integrity checks and whitelisting against PNT ICD	Under subcategory DS-6, add the following content to the second column Applicability to PNT: "Leverage PNT receivers that execute data integrity checks and white listing against the PNT system ICD as a desirable feature to protect against spoofing attacks."	Technical
	NextNav		42	541	4.2.6	Under PT-5, add further content to recommend use of PNT sources that leverge signals designed with inherent protection from diversity in time, frequency and/or code space.	Under subcategory PT-5, add the following content to the second column Applicability to PNT: "Use PNT sources that leverge signals designed with inherent protection from diversity in time, frequency and/or code space. PNT systems may be used that leverage encryption and authentication mechanisms for protection from cyber security attacks including data spoofing. PNT receivers can also gain protection from the use of cyclic-redundancy checks in data packets, the ability to discard measurements not associated with valid data, or for signals arriving outside expected windows of time. "	Technical
	NextNav		43	547	4.3.1	Detect anomalous behavior by cross-checking among different PNT sources	Add the following sentence to this section, for example in the first paragraph of 4.3.1: "PNT data from multiple sources may be used, cross-checked and compared for detection of anomalous behavior."	Technical

	NextNav		54	592	4.4.4	Expand on the use of alternate PNT sources in this paragraph. Leverage section 3.3.3 from the earlier draft.	Add section 3.3.3 from earlier draft as follows: "The ability to provide useable PNT data despite a compromise can be accomplished with technologies such as: • Atomic clocks (with a known holdover) • PNT diversity and segmentation • Alternative signals, such as other satellite constellations • Network-based solutions • Terrestrial RF sources (e.g: Terrestrial Beacon System [TBS]) • Signals of opportunity (such as cellular)"	Technical
	NextNav		67	792	References	Include references to ICD of other PNT systems beyond GPS	Add reference to MBS ICD as follows: "[MBS ICD] atis.org ESIF-ESM-2015-00038R001 Metropolitan Beacon System (MBS) ICD Version G1.0"	General
	NextNav		69	897	References	Include reference to TBS	Add reference to TBS as follows: "[TBS] 3GPP TS 38.305 NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN"	General