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

						Comment		Type of Comment
Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	(Include rationale for comment)	Suggested Change	(General/Editorial/Technical)
1	Orolia	John Fischer jfischer@orolia.com	14	457	AM-1	Consider adding IETF RFC 5905, NTP Ver 4 spec to the reference document list as part of identifying all ports that send or receiver PNT data. Or maybe that is not necessary. I see RFC 7384 – Security Requirements of Time Protocols in Packet Switched Networks, and RFC 8633 – NTP Best Current Practices, are referenced in other tables, maybe that is enough.		General
2	Orolia	John Fischer jfischer@orolia.com	23	471	GV-4	Consider the implications of using multi-GNSS receivers which obtain their data from foreign constellations in addition to GPS – Galileo (EU), GLONASS (Russia) and Beidou (China).		General
3	Orolia	John Fischer jfischer@orolia.com	26	485	RA-3	Consider GNSS vulnerability testing using GNSS signal simulators as another means to identify threats. Periodic testing is recommended. Consider a reference to this in Table 11, IP-10 also.		General
4	Orolia	John Fischer jfischer@orolia.com	34	518	DS-2	Consider referencing the new RFC 8915 Network Time Security for encryption/authentication of Time Protocol data		General
5	Orolia	John Fischer jfischer@orolia.com	36	518	DS-6	Consider protecting integrity by also subscribing to the CGSIC Bulletins (Civil GPS Service Interface Committee) and NOTAM (Notice to Airman) on GPS outages and activities.		General
6	Orolia	John Fischer jfischer@orolia.com	45	558	CM-1	consider noting that specialized detection HW and SW is available to detect GNSS jamming and spoofing events before they can corrupt the PNT data. Prudent users can implement these detection sensors. Some examples are here: https://www.orolia.com/products/interference-detection-mitigation		General
7	Orolia	John Fischer jfischer@orolia.com	47	558	CM-8	Vulnerability scanning should also include GNSS signal simulation for jamming and spoofing of the PNT equipment in either the actual system or in a System Integration Lab (SIL) so operations are not impacted.		General
8	Orolia	John Fischer jfischer@orolia.com	65	740	8633	first author's name misspelled: "Reilley" should be "Reilly" (he's one of our guys 😊)	Reilly	Technical