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 #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
DHS S&T 01	DHS	Ernest Wong / ernest.wong@hq.dhs.gov	20-21	BE-5	4.1.2	BE-5 has a lot of text. Does it all belong here, and at this level of detail? Suggest rewriting to make more concise and digestable.	See comment to left.	General
DHS S&T 03	DHS	Ernest Wong / ernest.wong@hq.dhs.gov	35	DS-6	4.2.3	DS-6: The DHS Best Practices document from 2017 uses the phrase "known good state" but the 2020 DHS RCF work has refined this to "proper working state" to avoid being prescriptive--restoring to a saved "backup" state (aka "last known good state") should not be the requirement.	Change "last known good state" to "proper working state" Also add footnote explaining the official change in language: "The 2020 DHS RCF refines the "known good state" concept to the more general "proper working state," which can included options other than a saved "backup" state."	Technical
DHS S&T 04	DHS	Ernest Wong / ernest.wong@hq.dhs.gov	35	DS-6	4.2.3	DS-6: The first paragraph is about a recovery capability rather than data security. This should be included in either RP-1 (execution of recovery) or IP9 (recovery planning, which ensures the capability is there).	Move first paragraph about rolling back to a good state / working state to Recovery RP-1 or Protect IP9. (see my comment regarding p.58).	Technical
DHS S&T 05	DHS	Ernest Wong / ernest.wong@hq.dhs.gov	36	DS-6	4.2.3	DS-6: The consistency check language (2nd to last paragraph) should also including validating PNT data inputs to protect against data corruption. This gets at the GPS whitelist for the navigation message. This is also from the DHS RCF.	1) Add "Protections should also be put in place to verify PNT input signals conform with service interface specifications and prevent internal data corruption." 2) Add reference to DHS RCF.	Technical

DHS S&T 06	DHS	Ernest Wong / ernest.wong@hq.dhs.gov	39	IP-9	4.2.4	IP-9: Having holdover and CPNT is not sufficient. Anomaly detection is needed to ensure the holdover device is not corrupted as well. Also added more system design considerations that align with responsible use of PNT.	Change "Include considerations for PNT source holdover and complementary PNT sources with dissimilar failure modes" to following: "As part of response planning, ensure your systems have mitigations to deal with PNT disruptions, to include (but not limited to) anomaly detection with holdover capabilities. If complementary PNT sources are used, mitigate common failure modes and ensure attack surfaces on new sources are mitigated. Downstream consumption of PNT information should also be restricted to the degree that is needed to limit the scope of response and recovery actions to PNT disruptions."	Technical
DHS S&T 07	DHS	Ernest Wong / ernest.wong@hq.dhs.gov	39	IP-10	4.2.4	IP-10 lists DHS RCF as a reference, but don't see any applicability language. IP-10 is about recovery testing, so there may be a thread there for applicability. I have a more general point of confusion on the CSF. There are Response and Recovery functions, but Response and Recovery activities also existing under the Protect function. Is the distinction that all planning and preparation for Response/Recovery is handled under Protect, and the Response/Recovery functions themselves are focused on execution of plans?	See comment to left.	General / Technical

DHS S&T 08	DHS	Ernest Wong / ernest.wong@hq.dhs.gov	42	PT-5	4.2.6	PT-5 references the DHS RCF but the applicability language should be expanded. Some of the existing examples are traditional concepts like holdover, which do not protect threats from entering your systems and is more of a response measure. Added language to expand the concept.	Replace existing text with following: "PNT mechanisms include proactive measures that reject bad PNT signals and data to limit how far threats penetrate into PNT systems. Reactive measures should also be present to handle threats that penetrate into PNT systems, to include holdover capabilities paired with anomaly detection, features to limit performance degradation, recovery capabilities. Resilience measures can also be achived through new system designs that limit exposure times to attack surfaces, protects internal states, and has intelligent control algorithms."	Technical
DHS S&T 09	DHS	Ernest Wong / ernest.wong@hq.dhs.gov	58	RP-1	4.5.1	Per my comment above on IP-10 (comment # DHS S&T 07), not quite sure where everything should go for recovery since it seems split across different functions, but suggest adding DHS RCF reference here since recovery is foundational to it and would also impact organizational actions.	Add DHS RCF reference to RP-1.	General / Technical
DHS S&T 10	DHS	Ernest Wong / ernest.wong@hq.dhs.gov				No doubt a lot of work went into compiling this, but has it gotten too complicated? The PNT Profile is very lengthy (50 pages of tables) and concepts are duplicated and/or split across multiple functions and subcategories. Are PNT users in critical infrastructure going to struggle with attempting to use this?	Highest level comment. See left.	General

DHS S&T 11	DHS	Ernest Wong / ernest.wong@hq.dhs.gov				I have some concerns on the scope and level of detail in the profile. Some parts of the profile get very detailed while others are less. And should it ever even get that detailed? Some areas are quite prescriptive about the development of mitigations, while also being incomplete mitigations (hence some of the earlier comments to flesh them out more). However, I think the scope of the document should be focused on asking concise questions that help users answer the question "are they using PNT in a responsible manner?" Does the document currently do that?	Next highest-level comment.	General
DHS CISA	DHS	james Platt, James.platt@cisa.dhs.gov	1	243		The recommended changes will focus the user on the supported system. There is little the user can do to protect the PNT system as this is provided by an outside entity	Modify to read/ "Protect systems that are dependent on PNT services by adhearing to the basic principles of responsible use. "	