From: "'Martin,Aaron K (BPA) - TEZP-AMPS' via pnt-eo" <pnt-eo@list.nist.gov>
Reply-To: "Martin,Aaron K (BPA) - TEZP-AMPS" <>
Date: Tuesday, November 24, 2020 at 6:56 PM
To: Katya Delak <>
Cc: "Li-Baboud, Ya-Shian (Fed)" <>, "Dodd Jr,Gary A (BPA) - JB-B1" <>, "pnt-eo@list.nist.gov" <pnt-eo@list.nist.gov>, "Christensen,Andrew L (BPA) -TEZP-AMPS" <>
Subject: [pnt-eo] RE: Draft PNT Profile Available for Comment

Hi Katya,

I apologize for not sending this yesterday. Below is feedback for the draft PNT profile from myself a s ubstation automation SME, a NERC CIP compliance engineer, and a cyber-risk specialist.

Below is the feedback from myself as a substation automation SME.

The "Asset management Subcategory AM-1: Physical devices and systems within the organization are inventoried" dives too deep into technical maintenance of PNT systems. Specifically the following s hould be removed from the document:

"The calibration of component delays (e.g., antenna, surge suppressors, cables, connectors, splitters , receivers, switches, etc.) should be recorded to optimize the absolute accuracy and/or relative precision in deploying systems that form and use PNT data. Delay variations and the stability of each component due to temperature or aging, should be characterized in the environment in which the PNT system will be deployed. Calibrations can be absolute or relative. Absolute calibrations are not biased by the calibration reference a nd would therefore be more reproducible. However, absolute calibrations can be more complex to de termine. The bias in relative calibrations would be consistent if all the devices in the system are calibrated a gainst the same calibration reference.
Particularly for applications that require traceability, document procedures for minimum periodic calibrations to a reference; after hardware updates, including FPGA code and firmware updates; and as part of the incident recovery plan. The frequency of calibrations is dependent on factors such as environmental conditions and PNT data performance requirements. Continuous time and frequency calibration services to UTC are also available."

This is important but should be relegated to the specific industry regulators such as NERC.

Below is the feedback from our transmission NERC CIP compliance engineer.

I’ve spent some time reviewing this and don’t have any specific feedback. It’s written very generically to cover anything from a cell phone company’s use of GPS for the end user’s mapping programs to industrial applications such as ours.
The document selects a subset of controls or requirements (from a larger set of national standards), and lists those that can be applied to protecting timing/navigation systems, and then adds some GPS-specific suggestions or guidelines.

In our case at BPA, many of the recommended controls won’t apply (for example, many of our GPS clocks aren’t network-connected and therefore aren’t automatically scanned for vulnerabilities), but many of the controls are covered by existing BPA processes (example: BPA’s maintenance program already includes regular maintenance for fault locators). Since the document provides flexibility to select the controls which make sense for each organization, I don’t have additional comments.

Below is the feedback from one of cyber risk specialist

The NISTIR 8323 Precision, Navigation, Timing (PNT) document is actually pretty good.

I don't have anything specifically to add other than it looks useful for scoping and tailoring controls at Transmission field sites where these types of devices are used. The Executive Order 13905 that prompted creation of this standard is long overdue in my opinion. This is based on the number of attacks targeting these types of services, being reported in the world, the last couple years. Further, based on the ABB Relay event from a few years back related to timing this type of standard and this type of work seems exceedingly important.

Please let me know if you have any questions.

Best regards,
Aaron Martin