The North American SynchroPhasor Initiative (NASPI) response to the NIST Request for Information: Profile of Responsible Use of Positioning, Navigation, and Timing Services[1]

The North American SynchroPhasor Initiative (NASPI) is a voluntary group of representatives from the utility industry, manufacturers and vendors, academia, national laboratories, government experts and standards-making bodies. The NASPI community is working to advance the deployment and use of networked wide-area time-synchronized electric power system measurements. NASPI areas of interest include synchrophasor data management and networking, engineering analytics, control room applications, transmission and distribution applications, performance requirements, and nurturing standardization and sharing of industry best practices. This collaborative effort is funded by the U.S. Department of Energy with support from the Electric Power Research Institute.

The NASPI responses to the RFI follow:

1. **Describe any public or private sector need for and/or dependency on the use of positioning, navigation, and timing, or any combination of these, services.**

The loss of GPS would impact most phasor measurement units (PMUs) deployed today, as they require time synchronization in the microsecond range. Most PMUs receive their time synchronization at the substation utilizing satellite clock receivers. If synchronization is lost or degraded, the accuracy of the measurements can be compromised.

(Source: Precision Timing Requirements in the Electricity Subsector PNNL-25984)

In addition, these precise timing sources may be used for logging disturbance data collection and its use for event analysis. Disturbance monitoring has a UTC ±2ms requirement for North American transmission utilities.

(Source: NERC Standard PRC-002-2 — Disturbance Monitoring and Reporting Requirements)

2. **Identify and describe any impacts to public or private sector operations if PNT services are disrupted or manipulated.**

An extended loss or degradation of GPS timing signals today would threaten some aspects of the real-time operation of the U.S. electric grid.

Some utilities have elected to include the results of measurements made by phasor measurement units (PMUs) in the operation of their control rooms. Since the PMU itself is dependent on precise timing, loss of this timing would mean loss of that capability in the control room or in system operations. For this reason, the North American Electric Reliability Corporation (NERC) regards some PMU-enabled applications as critical infrastructure, and they come under the purview of the NERC critical infrastructure protection requirements.

[1] A Notice by the National Institute of Standards and Technology on 05/27/2020, Document Citation 85 FR 31743

In addition, precise timing is a key requirement to enable accurate post-event analysis. The sequence of events of a major disturbance can often include a number of events occurring in rapid succession, and properly interpreting cause and effect of various automated controls requires accurate and precise logging of events. When a system event occurs (either electrical or cyber security), the exact sequence of events surrounding it is reconstructed from information stored in control rooms, data archives, fault recorders, syslogs, intrusion detection systems, and so on around the system. The availability of a distributed precise time reduces the challenges associated with reconstructing and understanding the sequence of events.

Without the precision of the distributed time signal, the sequence of events could still be reconstructed, but the reconstruction would become a process that occupied considerably more time (possibly months instead of days) and consumed many more resources. (Source: Precision Timing Requirements in the Electricity Subsector PNNL-25984)

3. **Identify any standards, guidance, industry practices and sector specific requirements referenced in association with managing public or private sector cybersecurity risk to PNT services.**

Applicable standards include:

- IEEE Standard C37.118.1-2011 for Synchrophasor Measurements for Power Systems defines synchrophasors, frequency, and rate of change of frequency (ROCOF) measurement under all operating conditions. It specifies methods for evaluating these measurements and requirements for compliance with the standard under both steady-state and dynamic conditions. (Source https://standards.ieee.org/standard/C37_118_1-2011.html)
- IEEE Standard 1588-2019 for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems defines a protocol enabling precise synchronization of clocks in measurement and control systems implemented with technologies such as network communication, local computing and distributed objects. (Source https://standards.ieee.org/standard/1588-2019.html)
    - IEEE Standard C37.238-201 Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications is a common profile for the use of PTP of IEEE Std 1588-2008 in power system protection, control, automation, and data communication applications utilizing an Ethernet communications architecture is specified. (Source https://standards.ieee.org/standard/C37_238-2011.html)
    - The IEEE 1588 Power Profile Certification Program provides the power industry with a means of confidently implementing the IEEE 1588TM-2008 Precision Time Protocol (PTP) in the electrical grid. PTP is capable of establishing a common time reference and synchronization across a system for realizing the applications that will ensure the reliability and resiliency of the grid of the future. (Source https://standards.ieee.org/products-services/icap/programs/ptp-power-profile/index.html)
- IEC/IEEE International Standard 61850-9-3-2016 Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation

specifies a precision time protocol (PTP) profile of IEC 61588:2009 ¦ IEEE Std 1588-2008 applicable to power utility automation, which allows compliance with the highest synchronization classes of IEC 61850-5 and IEC 61869-9. (Source https://standards.ieee.org/standard/61850-9-3-2016.html)

4. **Identify and describe any processes or procedures employed by the public or private sector to manage cybersecurity risks to PNT services.**

Prevention is the best course of action. Resilience can be achieved by designing redundancy into the needed grid control systems and in providing a backup source that is easy to activate.

The power industry is concluding that a system of redundant timekeeping should be installed in substations so that it can furnish time to all users within a substation. Some are already taking steps to implement this. In addition to or instead of GPS, some electricity subsector organizations rely on wide-area communications, such as Synchronous Optical Networking (SONET), that require wide-area precision timing. Others utilize an independent backup time source, such PTP (Precision Time Protocol), that can be used for clock synchronization over ethernet, and atomic clocks at substations.

(Source: Precision Timing Requirements in the Electricity Subsector PNNL-25984)

Other options for increasing time synchronization robustness include:

- Enhancing satellite-based timing systems
- Terrestrial radio-based systems, such as eLORAN (enhanced LOng-RAnge Navigation)
- Improved holdover oscillator accuracy
- Using products compliant with IEEE Standard 1588: Precision Time Protocol. PMUs self synchronizing the IEEE 1588 protocol and with the right network card can get better than 500ns, better than GPS.

Military grade clocks have had the luxury of anti-spoofing capabilities, typically through encrypted communications. In the last few years this capability has been made available to consumers as well. GPS firewalls block anomalous GPS signals and provide a hardened GPS signal output to downstream GPS systems.

(Source: https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall)

Utilities' Energy and Cyber security Program Plans should include protections of assets including PNT to ensure safety, availability, integrity, and confidentiality.

5. **Identify and describe any approaches or technologies employed by the public or private sector to detect disruption or manipulation of PNT services.**

Disturbance reporting (including relay action times) at the substation (local) level requires a high-precision timing measurement to verify that the equipment within the substation operated properly.

When a GPS signal is lost, holdover time is primarily provided by the internal system clock and is determined by the stability of the oscillator. Holdover time is the amount of time the clock can maintain precision without drift, which would compromise the accuracy of the time stamp on data coming from devices connected to the affected clock.

- A crystal oscillator will have a holdover of about 4 hours with a 1 millisecond drift. A (more expensive) rubidium oscillator will have a holdover of 4 days or more with a maximum drift of 1 millisecond.
- Quality of the oscillator is largely a function of cost.

(Source: Precision Timing Requirements in the Electricity Subsector PNNL-25984)

Maintaining the availability and integrity of the GPS signals is essential for ensuring correct estimation of phase angle measurements. Some of the recommended steps for allowing detection of suspicious activities are:

- Amplitude discrimination – Monitoring the observed absolute amplitude of the received signal for detecting any anomalies.
- Time-of-arrival discrimination – The time between the spoofed signals in case of most GPS satellite simulators is constant, unlike the time interval between true GPS signals.
- Angle-of-arrival discrimination – The angle-of-arrival (AOA) of GPS signals is monitored. Typical GPS receiver would receive signals from multiple GPS satellites with different AOAs, while in case of spoofing attack the AOAs will be the same.
- Cryptographic authentication – Information can be protected in transmission by using encryption and other message authentication schemes. Such schemes, however, need modification of the structure of the civilian GPS signals, which may take time.

(Source Time Synchronization in the Electric Power System https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf)

6. **Identify any processes or procedures employed in the public or private sector to manage the risk that disruption or manipulation to PNT services pose.**

Innovative technologies that use multiple timing sources are being implemented to maintain precise time when GPS disruption occurs. For example, new clocks can track both GPS and GLONASS signals, along with a remote PTP signal, to provide redundancy in timing sources. Terrestrial Time Distribution (TTD) systems can be used to mitigate GPS signal disruptions and maintain high-accuracy time synchronization across a wide area using such communications such as SONET.

Another method is using multiple GPS clocks, separated by distance, to receive GPS signals simultaneously. For example, one vendor's solution to manage the risk to disruption of GPS and time services, Schweitzer Engineering Laboratories (SEL) has a low-cost IRIG-B selection system (using the SEL-3400 IRIG-B Distribution Module) that can reliably perform the function of selecting the best IRIG-B source based on time quality or the loss of time signals. This device, along with a GPS clock, such as the SEL-2488 Satellite-Synchronized Network Clock, can reduce risk and monitor health of the signals. The

use of multi-constellation GNSS Receivers such as the SEL-2488 Satellite-Synchronized Network Clock, simultaneously tracks both GPS and GLONASS constellations and independently extracts time signals providing redundancy to prevent disruption or loss of services. (Source https://selinc.com/solutions/sfci/power-system-risk-mitigation/gps/)

Other satellite clock vendors have made similar advancements to increase the robustness and security of their timing signals. Examples include but are not limited to the General Electric RT430/RT434 GNSS Grandmaster Clock that is referenced to GPS and GLONASS satellites (Source https://www.gegridsolutions.com/measurement_recording_timesync/catalog/rt430.htm), Arbiter Systems Model 1200B GNSS Synchronized Clock that has multi-system timing sources (GPS/ GLONASS/Galileo/BeiDou) with multiple levels of security (Source https://www.arbiter.com/about-us/history-of-precision-time-experts-arbiter-systems.php), and Microsemi SyncServer S650 with multi-GNSS constellation support for enhanced reliability (Source https://www.microsemi.com/product-directory/gps-instruments/4135-syncserver-s650).

7. **Identify and describe any approaches, practices, and/or technologies used by the public or private sector to recover or respond to PNT disruptions.**

Utilities that have a Response and Recovery plan, as part of their Energy and Cyber Security Program Plans and regularly test, using their own or other testing options, are more likely to respond quickly and recovery robustly. NERC's GridEx, DOE's regional energy assurance exercises, and DHS's CyberStorm are examples of opportunities to simulate disruption and test response and recovery plans and increase awareness of these PNT vulnerabilities. Presentations on the threats posed by GPS spoofing have been presented at NASPI work group meetings to raise awareness of these issues.

The NERC Electricity Information Sharing and Analysis Center (E-ISAC) gathers and analyzes security data, shares appropriate data with stakeholders. The E-ISAC, in collaboration with DOE and the Energy Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electric industry and enhances industry's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents. The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by DOE and industry and managed by the E-ISAC, providing bi-directional cyber risk information sharing.

Utilities that are stakeholders in the E-ISAC can share data, receive back aggregated analysis and implement the best practices provided to help mitigate, respond and recovery quickly. (Source https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity)

Utilities submit DOE OE-417 forms (Electric Emergency Incident and Disturbance Report) with information on electric incidents and emergencies. DOE uses the information to fulfill its overall national security and other energy emergency management responsibilities, as well as for analytical purposes.

DHS also provides response and recovery assistance and supports DOE as part of FAST Act (Fixing America's Surface Transportation Act) of 2015. DOE coordinates energy sector crisis state activities with DHS, the Department of Justice (DOJ), the intelligence community, the national laboratories, and other

interagency partners. (Source Assessment of Electricity Disruption Incident Response Capabilities https://www.energy.gov/downloads/report-strengthening-cybersecurity-federal-networks-and-critical-infrastructure)

8. Any other comments or suggestions related to the responsible use of PNT services.

The future grid will have greater need for precision timing due to the implementation of smart grid technologies and the need for accurate time stamping of transactions, increased use of renewable energy sources that are switched in and out at various times, the need for enhanced diagnostics to help with event forensics, and the possibility of real-time, perhaps autonomous, operation.

Few applications will require better than the microsecond-level accuracy that GPS now offers, although the accuracy will need to be improved to 100ns to enable use of high-speed protective relaying applications such as traveling wave fault detection and location technology.

The primary resilience challenge in the future will be ensuring the availability and integrity of the timing signal as applications begin using real-time control schemes (e.g., synchrophasors used in remedial action schemes).

(Source: Precision Timing Requirements in the Electricity Subsector PNNL-25984)