(U) Subject: Department of Energy (DOE), Office of Electricity (OE), Response to NIST Request for Information (RFI) about Profile of Responsible Use of Positioning, Navigation, and Timing Services

(U) Date: July 10, 2020

(U) Background:

(U) Executive Order 13905 - Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services, was issued on February 12, 2020. The purpose of the E.O. was to engage the public and private sectors to identify and promote the responsible use of PNT service such that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure.

(U) Definitions within the E.O.:

(U) PNT Profile: A description of the responsible use of PNT services — aligned to standards, guidelines, and sector-specific requirements — selected for a particular system to address the potential disruption or manipulation of PNT services.

(U) PNT services: Any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.

(U) Responsible Use of PNT: The deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.

(U) The E.O. laid out the requirements for developing and reviewing PNT profiles in Sec. 4(a):

(U) Within 1 year of the date of this order, the Secretary of Commerce, in coordination with the heads of SSAs and in consultation, as appropriate, with the private sector, shall develop and make available, to at least the appropriate agencies and private sector users, PNT profiles. The PNT profiles will enable the public and private sectors to identify systems, networks, and assets dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services. Once made available, the PNT profiles shall be reviewed every 2 years and, as necessary, updated.

(U) The National Institute of Standards and Technology (NIST) has been tasked by The White House Office of Science and Technology Policy (OSTP) to develop a foundational PNT profile for the public and private sectors. The NIST approach will be using the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).

(U) To that extent NIST issued a request for information (RFI) on May 27, 2020 to seek “information about public and private sector use of positioning, navigation, and timing (PNT) services, and standards, practices, and technologies used to manage cybersecurity risks, to systems, networks, and assets dependent on PNT services.”

(U) Approach:

(U) DOE-OE forwarded the Power Marketing Administrations (PMAs) and various national laboratories that have expertise in PNT issues. Receiving this feedback DOE-OE consolidated the responses below.

(U) The RFI questions and consolidated response.

1) **(U) 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.**

(U) Response: The electric subsector typically uses PNT for synchronizing the internal clocks of Information Technology (IT) / Supervisory Control and Data Acquisition (SCADA), Substation, and Operational Technology (OT or telecommunications) equipment. The subsector also uses PNT for identifying the physical location of assets and resources.

(U) The basic functionality of the grid itself—synchronous generators interconnected with vast regional grids—does not directly rely on precise time in order to operate. The disruption of Global Positioning System (GPS) timing signals would not prevent today's grid from operating efficiently and reliably. The grid will continue to function, albeit with the possibility of confusion and corrupted data logs, regardless of the accuracy of the various time references that are being used today.

(U) The loss of GPS would impact phasor measurement units (PMUs) the most, as they require the highest timing accuracies (microsecond range). Most PMUs receive their time synchronization using GPS clock receivers. If GPS synchronization is lost, they can rely on internal clocks for a short period of time. Another application, while not yet in widespread use, require GPS-enabled precision time to support protective relaying applications. Other applications, such as event disturbance recording and cyber security forensic investigations, have timing needs and inaccuracies in time stamps could cause errors in aligning data and in forensics of disruptive events. (Source: Precision Timing Requirements in the Electricity Subsector PNNL-25984)

(U) The loss of GPS timing signals can also degrade control center operations such as time-tagging events, disturbance data collection and its use for recording events. Furthermore, this data may be used for playback in dispatcher training simulators. (Source: NERC Standard PRC-002-2 — Disturbance Monitoring and Reporting Requirements)

(U) PNT services are used extensively through the power system for a variety of different purposes including the following applications:

- (U) Traveling Wave for Fault Detection and Location for transmission lines time aligns high sampled data to record a transient signal resulting from fault on a transmission. Precise time allows the device to provide a precise location to the fault by calculating the distance using the time and velocity of the signal.
- (U) Phasor Measurement Units are placed at various substations in a geographically large area. They collect voltage and current data, timestamp each sample and send it to back to a Phasor Data Concentrator (PDC) at a central location. At the PDC, all of the received data is aligned via their timestamp. PMUs are used for the following applications:

- (U) Wide Area Protection, Frequency Event Detection, Anti-Islanding, Droop Control' Wide Area Power Oscillation Damping' and System Modeling verification

- (U) Line Current Differential Relays detect faults on both ends of a transmission line. If they do not have a direct fiber connection between them, they are communicating over a communications channel that can present channel asymmetry. PNT services are used to timestamp current magnitude and phase angle data and send it to the other relay. This data from the local and remote relays are compared to determine if there is a fault on the line.

- (U) Sequence of Events Recorders (SER), timestamps alarms from a large number of sources within the substation. This data is critical for event analysis, especially for large blackout type of events. Relays and other end devices can have their own SER internally for timestamping of digital events.

- (U) Digital Fault Recorders (DFR), records synchronized power system signals from a large number of analog sources within the substation. This data is critical for event analysis, especially for large blackout type of events. Relays and other end devices can have their own DFR internally for timestamping of digital events.

- (U) Substation Local Area Networks (IEC 61850 GOOSE and IEC 61850 Sample Values) rely on time synchronized data to perform automated functions including controlling power system breakers.

- (U) Time Division Multiplex equipment that cover a large geographical area used for power system communications rely on PNT services to synchronize their respective systems.

(U) The impact of a loss of time synchronization in electric utility communications has not been fully determined. Each utility will have their own unique approach to this issue as well as remedial actions. Developing PNT profiles that cover this area as well as the applications listed above could help in developing consistency in the approach and understanding the consequences of a loss of time synchronization in electric subsector communications.

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

(U) Response: To identify exactly the consequences of disrupted or manipulated PNT services is difficult because of the uniqueness in configuration of the many utilities in the electric subsector. In general, utilities' IT/OT and SCADA and systems can survive PNT service disruption for a time dependent upon the configuration of individual systems, geographic impact of PNT disruption, and quality of each PNT receiver's internal oscillator. Utilities IT/SCADA systems may be severely impacted by PNT service manipulation dependent upon the configuration of the individual systems, geographic impact of PNT manipulation, and the ability of the Network Time Protocol (NTP) to exclude false tickers. 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.

(U) 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. 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.

(U) 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.

(U) 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)

(U) With a disruption in PNT services, most power system devices will recognize that there is a disruption in timing and alarm as such. With a disruption, there isn't typically an adverse reaction, but reliability and functionality of these devices that support power system is degraded thus degrading the power system itself.

- (U) Transmission line fault detection equipment using traveling wave algorithms without PNT services will not be available to detect location of faulted or failed equipment for transmission lines. The impact would result in extend outages of transmission lines because manual discovery of the location of the failed equipment would be required.
- (U) Phasor Measurement Units that rely on PNT services would not be able to provide situational awareness over a wide area. This includes
    - (U) Loss of Frequency Event Detection and Loss System Modeling verification

(U) Also loss of the following wide area protection applications would be lost.

- (U) Loss Anti-Islanding, Loss of Droop Control, and Loss Wide Area Power Oscillation Damping

- (U) Time Division Multiplex equipment relies on PNT synchronization to function properly. Without PNT services, communication circuits, including transmission protection circuits, balancing of load across the grid, and remote indication and control of power system equipment would become unavailable resulting degradation of the power system.
- (U) Line Current Differential Relays dependent on PNT services. For a line differential relay with the timing disrupted, the differential will be disabled until timing is restored. The line differential would utilize less secure protection schemes.

(U) If PNT were to be manipulated the following applications could be adversely affected:

- (U) For PMUs, an adversary could either fake an event or mask a real one that is occurring. This could include islanding of the power system or forcing a Wide Area Protection scheme, such as Droop control or power oscillation damping to falsely operate.

- (U) For Line current differential relays, an adversary could force a transmission line to be taken out of service by manipulating the PNT service which would misalign shared data resulting in an indication of a false condition of the transmission line. This would lead it to take the transmission line out of service.
- (U) For SERs, an adversary could make it so the timestamps were incorrect with regards to event analysis. This would delay the investigation into the true cause of an outage.
- (U) For DFRs, an adversary could make it so recorded signals were not synchronized with the event. This would delay the investigation into the true cause of an outage.
- (U) Substation Local Area Networks (IEC 61850 GOOSE and IEC 61850 Sample Values) are integrated protection systems that rely on precise time to align data and take automatic operations. Precise time can be provided locally and there will be no impact as long as all equipment receives localized synchronized time and none of the schemes were integrated into wide area protection schemes or line differential schemes.

(U) It is important to restate the above consequences may or may not happen due to the configuration and security measures that may be in place. It is anticipated that defining PNT profiles that fit the above examples will likely lessen these consequences over a more generic profile.

(U) NTP packets are used for network synchronization, and often rely on GPS signals to synchronize the network onto the same clock. Should a loss of integrity occur (such as spoofing and/or corruption of an NTP packet) then clock signals could be changed.

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

(U) Response: DOE transmission entities follow the same requirements for IT systems (FISMA, NERC/CIP, NIST, etc.) to protect PNT referenced NTP servers. There are no known standards, guidance, industry practices, or requirements for managing cybersecurity risk to PNT services. WAPA OT systems follow utility industry guidelines as specified by NERC/CIP and WECC.

(U) Applicable standards include:

- (U) 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)
- (U) 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)
    - (U) 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)

- (U) 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)

- (U) 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)

3) (U) Identify and describe any processes or procedures employed by the public or private sector to manage cybersecurity risks to PNT services.

(U) Response: DOE transmission entities operate a mesh of geographically distributed and redundant PNT referenced NTP servers with secondary peering to other PNT referenced NTP servers, and tertiary internal backup oscillators. PNT referenced NTP servers are protected by the same cyber security controls as other IP based systems.

(U) 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 as network-based time synchronization e.g. NTP (network time protocol), or PTP (Precision Time Protocol), that can be used for clock synchronization over Ethernet, and atomic clocks at substations.

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

(U) Other options for increasing time synchronization robustness include:

- (U) Enhancing satellite-based timing systems
- (U) Terrestrial radio-based systems, such as eLORAN[1] (enhanced LOng-RAnge Navigation)
- (U) Improved holdover oscillator accuracy
- (U) 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.

[1] https://rntfnd.org/wp-content/uploads/eLoran-Definition-Document-0-1-Released.pdf

(U) 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)

(U) Utilities' Energy and Cyber security Program Plans should include protections of assets including PNT to ensure safety, availability, integrity, and confidentiality. The processes and procedures employed to manage cybersecurity risks include monitoring and controlling user access, and applying security patches.

4) (U) Identify and describe any approaches or technologies employed by the public or private sector to detect disruption or manipulation of PNT services.

(U) Response: 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.

(U) 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.

- (U) Quality of the oscillator is largely a function of cost with holdovers that range from single digit hours to days. (Source: Precision Timing Requirements in the Electricity Subsector PNNL-25984)

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

- (U) Amplitude discrimination – Monitoring the observed absolute amplitude of the received signal for detecting any anomalies.
- (U) 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.
- (U) 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.
- (U) 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.

(U) (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)

(U) Various manufactures of power system GPS receivers apply different methods to detect spoofing attacks including, proprietary algorithms, comparing PNT signals from GPS to GLONASS, and be having spatial diversity on the GPS antennas to detect a signal coming from an area that it shouldn't be and

locking the location (latitude and longitude) of the GPS receiver as once they're installed, they shouldn't be moving.

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

(U) Response: Most applications have some type of indication that there is a disruption in PNT services. For line differentials relays, the differential relay element is disabled when a loss of timing is detected. For PMUs, a flag is enabled in the output data stream so that downstream entities are aware of the loss of timing. DOE is investigating new technology that may manage the risk that disruption or manipulation to PNT services pose.

(U) 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.

(U) Spatial diversity is a means to provide assurance to the timing signal. One approach involves the use of multiple GPS clocks, separated by distance, to receive GPS signals simultaneously.. T Another approach simultaneously tracks both GPS and GLONASS constellations and independently extracts time signals providing redundancy to prevent disruption or loss of services. Both of these approaches can monitor the health and ultimatly increase the assurance of the timing signal.

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

(U) Response: Geographic redundancy, high quality internal oscillators, NIST Internet Time Servers.

(U) 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. Most entities will have basic recovery approaches to PNT disruptions that including call out of field personnel to investigate and replace a GPS clock in the event that it fails.

(U) 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.

(U) 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.

(U) 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)

(U) 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.

(U) 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)

7) (U) Any other comments or suggestions related to the responsible use of PNT services.

(U) Response: Many vendors have incorporated various constellations of GNSS such that issues with one constellation will cause a shift to another. Basically having a spaced-based PNT solution for a spaced-based PNT interference. However, as far back as 2014, the National Executive Committee for Spaced-Based PNT recommended eLORAN as a complementary PNT source. Six years later, in 2020, this remains a viable solution to interference of spaced-based solutions. What may eventually come are subscription services for time such as Iridium. However subscription services would need to have yet undeveloped industry standards. Given the sixteen critical infrastructures have different PNT requirements, and as described below that within the sector there will be different PNT requirements, national standards must be established for PNT beyond GPS. A PNT profile that addresses cybersecurity only will not address the quality or accuracy of the PNT signal.

(U) 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. There is currently an interest group that is being led by EPRI in regards to resilient timing that includes participation from end users, equipment vendors and government entities.

(U) 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. 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)

(U) Users and manufactures of PNT services need to be aware of the Federal Communications Commission (FCC) granting Ligado's Networks LLC's mobile satellite license modification application and the potential harmful interference to the GPS signals emancipating from Ligado's proposed low-power terrestrial nationwide network to be deployed in the 1526-1536 MHz, 1627.5-1637.5 MHz, and 1645.5-1656.5 MHz radio spectrum bands. As stated above, external interference of PNT signals would not be addressed by a cybersecurity only approach for PNT profiles.