Background:

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.

Definitions within the E.O.:

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.

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.

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.

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

> *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.*

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).

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*."

The RFI questions are as follows, there is a place for your responses to each question.

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.

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

- 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.

- 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:
    - Wide Area Protection
    - Frequency Event Detection
    - Anti-Islanding
    - Droop Control
    - Wide Area Power Oscillation Damping
    - System Modeling verification

- 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.

- 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.

- 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.

- 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.

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

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

Response:
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.

- 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.

- Phasor Measurement Units that relay on PNT services would not be able to provide situational awareness over a wide area. This includes
    - Loss of Frequency Event Detection
    - Loss System Modeling verification

  Also loss of the following wide area protection applications would be lost.
    - Loss Anti-Islanding
    - Loss of Droop Control
    - Loss Wide Area Power Oscillation Damping

- 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.

- 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.

With manipulation of PNT services, there can be substantial impact to the power system. If PNT were to be manipulated the following applications could be adversely affected:

- 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.

- 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.

- 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.

- 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.

- 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 non of the schemes were integrated into wide area protection schemes or line differential schemes.

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.

   Response: NERC CIP standards are applied to GPS receivers for critical power system applications.

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

   Response: The processes and procedures employed to manage cybersecurity risks include monitoring and controlling user access, and applying security patches.

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

   Response: 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.

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.

   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 datastream so that downstream entities are aware of the loss of timing.

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

Response: 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.

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

Response: 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.

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.

If you send to me your responses by COB June 8, 2020, I will reconcile all comments, resolve conflicting comments, and will submit a single DOE response to NIST by COB June 12, 2020.