Profile of Responsible Use of Positioning, Navigation, and Timing Services

Response from Satelles, Inc.
Agency/Docket Number: 200429-0124
Docket ID: NIST-2020-0002

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.

Satelles is an alternative PNT provider rather than an operator of critical infrastructure, but the company is keenly aware of the dependencies of the various sectors. Here are just a few examples of the needs of various critical infrastructure operators:

- **Wireless providers** rely on GPS for timing within each cell site within their macrocell, small cell, and femtocell networks. Without precise timing, these networks would not operate. The timing accuracy requirements for these network elements becomes even more critical with 5G.

- **Energy companies** rely on GPS for timing for their industrial controls, synchophasors, and a variety of networked elements connecting their facilities. The energy sector has been shifting their infrastructure to be more dependent on accurate timing, and the expectation is that this reliance on timing will become even more significant within the next five years.

- **Financial organizations** rely on GPS for timing within data centers, and each trade is highly dependent on very accurate timing references. Additionally, financial organizations rely on secure and accurate positioning for cybersecurity. This reliance has become more critical as the use of mobile devices are relied upon for financial transactions. (NOTE: Major stock exchanges in the United States and around the world are currently using STL for backup timing in their data centers.)

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

As the primary domain of PNT, GPS (and other GNSS) must be protected. Backup capabilities from out-of-domain PNT solutions such as STL are an essential safeguard for telecommunications networks, electrical power grids, transportation systems, and other types of infrastructure that rely on PNT to operate even if GPS is unavailable or degraded. STL delivers alternative PNT at the levels of stability, reliability, and trust required by commercial enterprises and government entities across a range of critical infrastructure applications. A few examples are provided below.

Wireless Carriers

Wireless communications networks around the world rely on accurate timing and synchronization from GPS (or GNSS) signals to function properly. The loss of GPS via disruption, manipulation, equipment failure, or spacecraft anomaly has been known to disable critical equipment, including macrocells, distributed antenna system (DAS) installations, and small cells.

LTE networks are particularly vulnerable to timing anomalies and often have timing requirements of one microsecond or better. The requirements of 5G are even more stringent. Single-tower timing errors outside of this range have the potential to disrupt communications over a broad local region, and a widespread outage of GPS could potentially render communications inoperable over entire nations.

For DAS and other in-building wireless installations, STL offers the added advantage of timing signals that penetrate most structures, including buildings with low-emissivity (Low-E) windows or metal and concrete siding and roofing. This means that in-building wireless installations that leverage STL can maintain synchronous timing without the need for an external GPS antenna. Femtocells — which are typically found in indoor locations where GPS is not available — also require precision location (to support emergency services) as well as timing, and STL offers both time and location for these devices.

Having a signal that passes through structures is especially important for buildings where securing roof rights, obtaining landlord permissions, or complying with local zoning restrictions are a challenge. An indoor solution for assured PNT also lowers cost and reduces the risks of installation and maintenance.

Electrical Grid

Energy suppliers and public utilities (electricity, oil, natural gas, water) that rely on precise timing for their operations can depend on GPS/GNSS augmentation or backup from Satellite Time and Location (STL), which is compatible with the Precision Time Protocol (PTP) / IEEE-1588 standard.

Every country's national electrical grid is becoming more vulnerable to hacking attacks as grid operators expand the use of phase synchronization and other smart grid techniques that rely on GPS/GNSS signals for timing. For example, synchrophasor systems utilize phasor measurement units (PMUs) for providing electrical power system reliability and grid efficiency, synchronizing services among power networks, and finding malfunctions within transmission networks.

PMUs rely on GPS to timestamp their measurements, which are sent back to a central monitoring station for processing. GPS manipulation could alter a PMU's timestamps, thereby causing a PMU to deliver erroneous measurements regarding power frequency reading and power flow calculations. Such a scenario would likely cause some elements to overheat as well as lead to overloaded lines or transformers, potentially causing blackouts or damage to power grid equipment.

Serving as a GPS timing and synchronization backup for electrical grid applications, STL provides trusted timing and synchronization for continued reliable synchrophasor operation when GPS signals are disrupted or manipulated.

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.

n/a – No response from Satelles

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

In our experience, one important way in which Cybersecurity risks are managed is by using an alternative source of PNT. For example, the Satellite Time and Location (STL) service from Satelles provides customers around the globe an accurate, secure, and reliable source of PNT using the Iridium low Earth orbit (LEO) satellite constellation. STL is unique in that its signals are powerful, extremely secure, and available worldwide. The high-power signals provide a backup to the Global Positioning System (GPS) as well as penetrate into GPS-challenged environments where signals are obstructed or degraded, including indoors. The complex, overlapping beam patterns of Iridium satellites combined with modern cryptographic techniques allow STL to deliver a trusted time and location capability that is highly secure.

Satelles offers assured PNT at levels of stability, reliability, and trust required by critical infrastructure and cybersecurity applications. With worldwide deployments, STL has the operational readiness that civil government officials and private sector leaders expect when ensuring uninterrupted access to PNT sources that strengthen the resilience of our national critical infrastructure.

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

The threat from disrupted or manipulated GPS signals is real. While Satelles does not provide any detection services, Orolia – *one of Satelles' partners* – offers a comprehensive array of Interference Detection & Mitigation (IDM) products and services, including one that works in tandem with the STL service.

Orolia's SecureSync Interference Detection Suite is a package of disruption and manipulation recognition algorithms available for its SecureSync receiver, a device that can be configured to use STL as an alternative form of PNT. When the SecureSync Interference Detection Suite software algorithms detect an anomaly with the GPS signal, the SecureSync can either shift to timing holdover based on a precise internal oscillator or automatically switch to an alternative timing reference such as STL.

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.

Satellite Time and Location (STL) is an alternative PNT solution utilized today by commercial entities that manage cybersecurity risks to PNT services. For example, several major financial institutions and stock exchanges around the world utilize STL today to provide secure timing in the event GPS is unavailable. The equipment recognizes the loss or lack of GPS signal and utilizes STL as the timing source without any interruption in service. This is vital to entities like stock exchanges where the security, integrity, and accuracy of time is critical to their business and our economy.

Additionally, due to the proximity of LEO satellites — 25 times closer to the Earth than GNSS satellites — and a high-power satellite signal, STL broadcasts are 1,000 times (30 dB) stronger than GPS, making them very difficult to disrupt or degrade. Additionally, the unique architecture of the Iridium satellite constellation combined with modern cryptographic techniques enable a proof-of-location approach that allows STL to deliver a secure, trusted time and location capability that is effectively impervious to manipulation.

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

n/a – No response from Satelles

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

The views of Satelles are predominately aligned with the findings of the *Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)* that the U.S. Department of Homeland Security issued to U.S. Congressional committees in April as required by National Defense Authorization Act for Fiscal Year 2017. Included below are specific concepts from the report (with relevant excerpts) that reflect the Satelles position.

Out-of-Domain Solutions and the Benefits of Low Earth Orbit Satellites

In its report, DHS notes that "critical infrastructure systems that would cease to operate without [the primary PNT domain of] GPS do so because of design choices, cost factors, increasing efficiency, or other considerations—not because of a lack of available additional means to navigate, determine location, or synchronize." As DHS goes on to say, "there are smart, market-oriented solutions that will contribute to enhanced resilience that the U.S. Government should continue to promote, enable, and stimulate."

GPS and other GNSS operating mostly in medium Earth orbit (MEO) are the primary domain for PNT services. Out-of-domain solutions such as low Earth orbit (LEO) satellites, terrestrial wireless infrastructure, network time transfer, signals of opportunity, and other technologies are required as an essential backup to preserve the operations of PNT-dependent systems and safeguard our national critical infrastructure.

STL from Satelles is an out-of-domain PNT solution in the LEO satellite category. LEO constellations have different operational features and performance characteristics than MEO systems in the primary domain, such as increased signal strength and improved satellite safety.

The benefits of a LEO-based solution such as that offered by Satelles include:

- **High Power Signals –** STL signals are sent using a unique high-power channel, which combined with the proximity of LEO satellites (compared to GPS satellites in medium Earth orbit) and signal coding gain, produces a signal that is 1,000 times (30 dB) stronger than any GNSS signal. Also, Iridium's cross-linked mesh architecture provides superior availability and reliable performance. The cross-links enable continuous satellite orbit and time calibration to provide consistent PNT performance from the entire constellation.

- **Continuous Signals from Everywhere in the Sky –** Iridium satellites travel at speeds of approximately 17,000 mph (an eight-minute horizon-to-horizon transit), resulting in carrier frequency variations due to Doppler effects. With satellites rapidly traversing the sky, the continuously changing signal allows the

transmission of STL to reach receivers in the most challenging locations. Furthermore, Iridium satellites' polar orbits ensure global coverage, including at the poles (where the GPS signal is weak).

- **Not Susceptible to Terrorist Attack –** Unlike land-based systems, satellite systems are effectively impervious to terrorist attack, and are far less vulnerable to state actor attack.

- **Protection from Space Phenomena –** At their lower orbit altitude, LEO satellites are well protected from space disturbances (e.g., solar storms), and they are far less susceptible to the deleterious effects of internal charging and surface charging that can cause permanent damage to the electronic components of space vehicles operating in MEO or GEO orbits. LEO satellites are better shielded from these phenomena because they orbit below the Earth's magnetosphere and inner Van Allen Belt (planetary radiation belt).

These attributes are relevant for those critical infrastructure owners and operators that depend on an alternative source of timing to back up or augment GPS.

Diverse Needs of Critical Instructure Sectors and Common Requirements Are Both Met by Alternative PNT

Each critical infrastructure sector has different needs, but there are certain baseline requirements. Satelles believes that a heterogeneous backup to GPS is in the public interest and also agrees with the report's statement that "DHS could not identify generic specifications for a national backup" because "[t]he position and navigation functions in critical infrastructure are so diverse that no single PNT system, including GPS, can fulfill all user requirements and applications."

In calling out some common specifications, DHS explains that "a minimal acceptable precision of anywhere between 65-240 nanoseconds […] supports all critical infrastructure requirements." The report states that this range "is expected to meet future requirements, including 5G." Based on the precision of timing references used by receivers, STL currently delivers timing accuracies between 50 to 240 nanoseconds, proving that it is one of the out-of-domain solutions ready to meet timing requirements that strengthen the resilience of critical infrastructure.

Critical Infrastructure Owners and Operators Need More Than a Single Form of Alternative PNT

The Federal Government should neither provide nor select a single PNT solution; rather, it should encourage diversity and invest in multiple technologies. With regard to any kind of government preference for a particular PNT system, DHS states that "the government would have to consider the repercussions of such a system in the marketplace" because "[a] free government system would negatively impact commercially available PNT systems by directly competing with them."

Satelles maintains the view that a truly resilient and globally available GPS backup capability is only possible with an open, technology-neutral approach that encourages diversity. Furthermore, Satelles agrees with DHS that "[t]he Federal Government should encourage adoption of multiple PNT sources [by] critical infrastructure owners and operators [and] focus on facilitating the availability and adoption of PNT sources in the open market."