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 financial market uses precise time to find the “best” price for securities, enforce fair trading, and conform to SEC and FINRA rules and regulations.

The public safety and emergency response (e911) require precise time to properly dispatch police, fire, ambulance and other services and to legally prove that the response was done in a timely manner or according to e911 regulations.

Precise time is required for information cybersecurity to properly authenticate users and systems. It is also required to trace cyberattacks through complex network-leveraged tactics.

Many other time-critical network applications exist, such as DoDIN, data center, OTT broadcast, wireless 5G IoT, power utility synchrophasors, fair online gaming, systems automation, and more.

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

In the financial sector: Microsecond errors could lead to trading at adverse prices, impacting retirement and other funds. Front-running, spoofing, quote stuffing, and similar activities would go unnoticed.

In the public safety and emergency response (e911) sector: Potential mis-dispatch of emergency equipment. Coordination errors because expected availability of resources was incorrect. Exposure to lawsuits because of false time, including causes that units were dispatched late or arrived late.

In the information security sector: Enables cyber-exploits like Kerberos replay attacks. Prevents tracing the flow of an exploit throughout a system.

In the broadcasting sector: Poor “lip sync”. Improper insertion of advertisements leads to revenue loss.

In the wireless telecom/5G sector: Total loss of communications at worst, lesser effects result in poor voice and video quality.

In the power utility sector: Time synchronization of syncrophasers for greater efficiency. Generators not able to connect to grid. Possible harm to generating devices.

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.

Financial standards: SEC 613, FINRA 4590, MiFID II, and others.

Telecom/5G standards: various ITU-T Gxx sync standards

e911 standard: NENA NG9-1-1 i3

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

Patented FSMTime’s TimeKeeper SkyMap technology: analyzes GNSS signals for cyberattacks, such as spoofing and jamming, and provides mitigation techniques.

Patented FSMTime's TimeKeeper Active Client technology: Uses signals from many time sources (including GNSS, PTP, NTP and others) to verify (determine correctness) and validate (trace to a reliable source) time. Can self-heal a time network by mitigating cyberattacks and detected time errors.

Patented FSMTime's TimeKeeper Compliance technology: monitors time accuracy over many clients to help detect and mitigate where cyberattacks may have occurred.

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

See the above item 4.

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.

See the above item 4.

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

See the above item 4.

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

Great NIST RFI initiative for gathering the above information from all the PNT players.