Cory Palmer
International Business Machines
NIST-2020-0002

"Profile of Responsible Use of PNT Services"

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. GPS/ SATPHONE / GIS Systems

As we continue to become a globalized world not only in commercial related activity, but in technology, we must recognize that PNT risks associated with Global Positioning Systems, Satellite Phones and Geographic Information Systems are pertinent and potentially susceptible to a cyber-attack. A denial of GPS, or a risk to secure SATPHONE communication and/or a misplaced latitude/longitude/MGRS/UTM as it relates to targeting efforts around the world for example are critical to understand and prevent.

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

There are many ways in which public or private operations can be disrupted or manipulated given compromised PNT. Ones that represent undue harm to public and private operations include: airplanes being in the wrong airspace, Power Grids shut down, trains on the wrong track, population centers off track for traffic signaling. These examples and more should be recognized as an immediate concern.

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.

An example associated with managing public or private sector cybersecurity risk to PNT services include, but not limited to, PKI encryption, data security and access. Fundamentally, PNT relies on security and systems, both of which can be considered a risk especially if compromised.

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

IBM software and platforms like Guardiam Data Encryption, KLM and MaaS360 are integrated platforms that are used widely the public and private sector to provide security around people, data and devices.

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

A few technologies employed by the public or private sector to detect disruption or manipulation of PNT services include: Gossimer (Gossimer LLC), Stingray (Harris), DRT (Boeing).

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. **One process that can be potentially be used to help manage the risk and manipulation of PNT Services is the red/black encryption concept.**

7. Identify and describe any approaches, practices, and/or technologies used by the public or private sector to recover or respond to PNT disruptions. **Mirror link Technology, Matrix Switching, Band Differentiator.**

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