Regulus Cyber welcomes the opportunity to assist NIST in the creation of a foundational PNT User Profile by sharing knowledge gained from Regulus' activities as technology provider in the field, particularly in the context of GPS/GNSS cybersecurity.

Based on our in-depth knowledge of GPS anti-spoofing technology, our recommendations and comments emphasize minimizing the threat of malicious manipulations of GPS frequencies to spoof and fake time and/or location information received by GPS receivers. While suitable solutions will need to be more precisely defined on a sector-specific level, we recommend that the foundational PNT User Profile includes the following considerations:

To harden critical infrastructure systems and promote the responsible use of PNT, measures against the effects of GPS cyber attacks such as spoofing must become part of our system's architecture. Undetected spoofing attacks can cause severe consequences and harm national and public safety (e.g. disruptions of the communications network that affect Emergency Services, and manipulation of Offender Tracking Devices). For this reason, resiliency against these acts must be addressed as part of the foundational User Profile and further investigated and defined by sector-specific agencies.

In addition, attack methods have rapidly evolved in the past years, making spoofing attacks feasible and achievable. With Software-defined Radios and open source based code, systems in all sectors can be made vulnerable to spoofing. In the second part of this document we will discuss different use cases and vulnerability tests of PNT-reliant systems, all of which were attacked using cheap and openly available hardware as well as open source based code. Due to the increasing accessibility of the necessary hardware, software and instructions, the growing likelihood of spoofing attacks must be taken into account as part of risk assessment. Furthermore, in our extensive testing of systems including mobile phones, automobiles with varying levels of ADAS and autonomous features, electronic monitoring/offender tracking devices, drones, and high and low-end GPS receivers used for synchronization purposes and critical infrastructure sites, we have yet to encounter a system that is resilient against these low-cost spoofing attacks.

In general, we recommend a deterministic approach towards this cybersecurity threat that allows for precise decision-making in case of attempts to disrupt critical infrastructure sites and therefore national safety. This effectively means that while back-up and holdover systems are important measures when implementable, the knowledge of an attack taking place on a critical infrastructure site is of equal importance.

At the same time, we must consider economic and practical factors in order to not unnecessarily burden the respective industries. Depending on the sector, supplementing sites with a number of added hardware components may not be feasible, nor may it achieve the

goal. Instead, the sector-specific risk analysis must draw realistic conclusions to determine the risk and the best way to implement suitable security measures against GPS spoofing attacks.

Depending on the sector and the platform using PNT, different types of approaches to secure the system from GPS spoofing attacks may be considered. Useful risk assessment questions for spoofing attacks include:

- Is my system a static or moving target?
- How many attack points (i.e. GPS receivers) does my system have?
- Does my system use GNSS data for timing and/or location information?
- Does my system use sensor fusion to determine time and/or location information?
- Is my system capable of distinguishing which sensor is offering correct data in case a conflict is detected?
- Is my system able to recognize if an attack is taking place in case a conflict is detected?
- Which kind of attacks can my system identify?
- Does my system require active mitigation technology? Does it have backup and holdover systems in place?
- From an economic and practical perspective, does my system allow for added hardware? What are alternative software solutions?

Impact of GPS spoofing attacks on sectors and systems depending on PNT.

Sectors that depend on resilient and authenticated PNT information include but are not limited to the Emergency Services Sector (EES), the Communications Sector, the Transportation Systems Sector, the Energy Sector and the Financial Service Sector. Aside from the different use cases of PNT, the integration of GPS within networks and system architectures differs greatly between sectors and has a direct impact on risk assessment and risk strategy.

In the Communications Sector, targets (cell towers and base stations with GPS) are static and may offer a bigger space to add hardware detection and mitigation technology. However, the amount of targets is significantly higher than in the case of power plants (Energy) and stock markets (Finance), which must be taken into consideration when implementing protective technology.

In EES and Transportation, GPS is often part of non-static platforms and the amount of targets is significantly higher than in other sectors. This also generates economic considerations and affects the physical space that can be allocated for security technology.

The Emergency Services Sector uses PNT to locate and navigate law enforcement, fire and emergency services, medical emergency services, search and rescue, and other tactical teams or aviation units such as police helicopters. As mentioned above, GPS plays a vital role in law

enforcement and the corrections technology field – it allows targets and individuals to be monitored and tracked in order to preserve public safety. Due to the critical use of GPS as one of the core technologies for offender tracking systems, responsible use of PNT and security measures against GPS spoofing attacks are of immense importance.

Electronic Monitoring Devices are frequently used for activities such as pretrial supervision, monitoring of juvenile defendants, victims of domestic violence, probation and parole, and counteracting overpopulation in prisons, the latter becoming of increased urgency due to the COVID-19 pandemic. Accordingly, in order to fulfill the requirements of the health department, many inmates had to be released prematurely equipped with GPS-reliant ankle monitors.

Unlike in the communications sector, GPS offers many useful tools and functionalities to correction and law enforcement agencies that are predominantly based on location. Officers can monitor and track a person's whereabouts, set up alerts if certain "off-limit" areas are accessed, and backtrack the movements of an individual. A trustworthy GPS tracker is necessary to rule out false positives, enabling officers to identify actual attempts to circumvent the device and prevent violations.

As GPS spoofing introduces an inherent GPS vulnerability across industries and systems, one must acknowledge the negative effects spoofing can have on monitoring devices. Examples include allowing an offender to enter prohibited areas without triggering an alarm or manipulating location data in order to avoid being backtracked to a crime scene. GPS data can already serve as evidence in a court of law, with its reliability being a key factor in this context. Due to the essential role that GPS plays for electronic offender monitoring, the negative results of spoofing must be addressed, and protections must be put in place against it.

In order to test the premise that electronic monitoring systems may be susceptible to spoofing attacks, our red team made an initial assessment of the technology by enacting a simple spoofing scenario. We acquired an ankle monitor with GPS tracking and geofencing capabilities and checked if the wearer of the device could leave the fenced zone without triggering an alarm. When attempting to leave the designated area, the ankle bracelet alerted the system immediately, exposing the wearer of the device. We then had the wearer activate a self-made spoofing device based on instructions available on the Internet and accessible to everyone. As soon as the wearer started to generate false signals, he was able to leave the area without triggering an alarm.

The initial performance of our Red Team confirms the vulnerability of Electronic Monitors to GPS spoofing hacks. Electronic Monitors are susceptible to GPS spoofing attacks, giving unauthorized freedom to offenders and potentially endangering the public. The rise of homemade spoofing devices with readily available instructions on the Internet magnifies this threat. Additionally,

monitored offenders have a high level of motivation and a strong incentive to manipulate their tracking devices and location.

These kind of use cases must be addressed as part of the effort to create responsible PNT user profiles.

The Communications Sector relies heavily on GPS for timing and synchronization purposes. Synchronization requirements are becoming increasingly stringent to support new technologies, advanced LTE and the 5G network. Ultra-high data rates and bandwidth require telecommunications providers to deploy a robust synchronization plan for their networks to provide uninterrupted service and support safety critical communication (ESS) and new technologies. In order to maintain a resilient network, providers combine different technologies within their system architecture. Network Timing Protocol and Precision Timing Protocol enable packet-based synchronization, which is particularly useful for timing synchronization between small cells and sharing of the timing source with another base station in close proximity. In addition, atomic and rubidium clocks enable holdover capabilities for the network in case there is no real time GPS signal available as a timing source. This use of technology creates redundancy but does not provide exclusive protection against cybercriminals that may generate distorted or fake satellite signals and disrupt services.

It is therefore necessary to implement dedicated technology to secure networks from spoofing attacks. Several companies in this field are developing and offering different approaches to solve this problem, some with added hardware, a combination of hardware and software, or a pure software solution. The suitability of these approaches will depend on the evolving system architecture of cellular networks regarding the implementation of 5G. One of the core points to assess the spoofing risk and strategy for the telecommunications sector is the amount of GPS receivers deployed within the network, indicating whether hardware or software technology is more economical and efficient to detect spoofing attacks.

Furthermore, it must be considered what kind of spoofing attacks can be and need to be detected. In an experiment conducted by our red team, we concluded that contrary to popular belief, accurate 1PPS Spoofing can be accomplished using inexpensive hardware and open source software, eliminating dependency on high-end and costly RF simulators. Using a $100 GPS disciplined oscillator, a slow drift of the clock with perfect 1PPS alignment was demonstrated on a receiver used for timing and synchronization of telecommunication networks. The research exposes a vulnerability that can be exploited by hackers to disrupt networks and services.

Recent interruptions in the network of one major communications provider showcased the importance of a resilient architecture. Cyber attacks like the spoofing of GPS signals can cause major network disruptions and denial of service.

In this context, the communications sector is closely connected to the **emergency services sector,** which relies on a stable network in order to support emergency calls, first responders, law enforcement and even correctional technologies like ankle monitors that build on robust GPS, cellular and Wi-Fi connectivity.

In more future-oriented scenarios, disruptions in the communications network can have massive impacts on smart cities and connected services, extending from mass transportation systems to mobility and location-based services.

In the Transportation Sector, GPS is an important component for the positioning and navigation of mass transit systems, aviation, highway infrastructure, motor carriers and more.

GPS is widely used for Electronic Logging Devices (ELD), which are mandatory for commercial vehicles to ensure responsible driving hours and breaks. Through GPS spoofing methods, many of these devices can be manipulated and potentially put drivers and their environments at risk. A scenario that needs to be considered in this case is self-inflicted spoofing that may be performed by drivers themselves in order to complete their work in the demanded time.

Furthermore, we conducted extensive research and testing on vehicles with varying degrees of ADAS and autonomous features. GPS is one of the major sensors used in many advanced driving systems and is utilized as part of the sensor fusion process. During our experiments we detected safety compromising behavior when GPS was spoofed. This problem is estimated to become more critical with the advancement of autonomous vehicles, specifically considering the use of autonomous trucks. Early steps towards responsible use of PNT within vehicles that are using ADAS and autonomous features are therefore highly recommended.

In addition, GPS is a core technology for tracking, including the tracking of hazardous materials that are being transported by different means of transportation.

Drones and other aerial vehicles deployed to monitor borders or critical sites rely on GPS for their operations.

In the maritime industry GPS is a core technology to navigate ships as well as vehicles in the port and even offshore drilling platforms.

For the Energy and Financial Services Sector precise timing is of extremely high importance with GPS being one of the technologies used for accurate timing and synchronization of core services. Due to the stationary nature of most systems in both sectors, a combination of many different methods is used to make the PNT system resilient and reliable. Important and useful strategies – including the deployment of decoy antennas, blocking sensors, obscure antennas – have and will be proposed by other official working groups and shall not be repeated in this document.

The importance of responsible use of PNT technology in these sectors is evident when considering the possible outcomes and consequences of a failure caused by a cyber attack:

- Financial Institutions like the stock market could be shut down or even manipulated if the system is spoofed without triggering alerts.
- Energy facilities may be disrupted, resulting in a shutdown of services with catastrophic outcomes for infrastructure and public safety.

In these facilities the detection of an ongoing spoofing attack is of equal importance to the mitigation of such and must be communicated to the relevant sectors on a real-time basis.

About Regulus Cyber

Regulus Cyber is taking a holistic cyber approach to address GNSS vulnerabilities by offering a software-only protection (like an "anti-virus") for GNSS, providing location and time integrity under a wide range of ever-evolving attacks and attack surfaces.
Regulus Pyramid GNSS is a software library for detection of cybersecurity attacks and authentication and protection of GNSS. It is readily compiled into any required target, lightweight and easily integrated anywhere in the system, whether new or retrofitted, and has both connected and stand-alone operation options to fit different use cases. Its flexibility of integration modes and low footprint are critical for securing mobile phones and embedded IoT applications.

Regulus Cyber is also developing a complementary, patent-pending, cybersecurity spoofing mitigation technology to make GNSS receivers resilient to attacks. Proprietary algorithms incorporate spoofing classifications and tracking techniques into a software-based GNSS receiver to keep it accurate and operational, even while under cybersecurity spoofing attacks.
To achieve the high level of protection provided by the Pyramid GNSS technology, Regulus Cyber has developed world leading GNSS spoofing attack capabilities. Regulus Cyber has 100% success in spoofing GNSS receivers, chipsets and systems, high and low-end devices, mobile phone platforms and high-end secured automotive positioning systems. Creating ever-evolving cybersecurity attack capabilities has enabled Regulus to develop expertise with real-world attacks, providing a key differentiator that gives our software solutions a clear and unique edge over competitors.
Regulus Cyber's Pyramid GNSS software is ready and being deployed across multiple industries worldwide.