

Recommendation for Committee Decision

Prepared by: Working Group S
Date of Submission: 13 October 2022

Issue Title: Incorporating Resilience into GNSS Interference Detection and Mitigation

Background/Brief Description of the Issue:

Modern Multi-PNT (Positioning, Navigation, and Timing) Ecosystems are facing new trends, new challenges, and an emerging paradigm that creates a need to incorporate resilience into GNSS Interference Detection and Mitigation (IDM). With increased attack surfaces and the proliferation of technology and know-how, end-users will need to operate with the expectation of an increasing frequency of PNT disruptions. Spectrum protection of GNSS services and enforcement by the spectrum regulators, as well as detecting, locating, attributing, and removing sources of interference are necessary, but not sufficient to address real-time operational needs. End users of PNT systems will need to be prepared to expect interference and have the ability to withstand, operate through, and recover from disruption events. Both external and on-device IDM capabilities will be important to enable resilient response. Broader changes involving resilient system architectures and operational resilience will be essential as well.

Discussion/Analyses:

These new challenges will require development of new government policy to ensure that disruption or manipulation of PNT services does not undermine the liable and efficient functioning of its critical infrastructure. Governments must also increase their own nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and must ensure critical infrastructure can withstand disruption or manipulation of PNT services. To this end, national governments are encouraged to protect GNSS spectrum from interference, implement IDM capabilities, and engage the public and private sectors to identify and promote the responsible use of PNT services. National governments should also emphasize the importance of resilient PNT system architectures, including the incorporation of cybersecurity principles into their design.

Recommendation of Committee Action:

To increase critical infrastructure resilience to GNSS disruptions and interference, the ICG recommends that the ICG members should consider the reinforcement of their IDM policy based on a three-prong approach: 1. (Service Aspect): National GNSS spectrum protection and enforcement and implementation of IDM capabilities; 2. (Hardware Aspect): PNT systems designed with resilient system architectures and systems incorporating cybersecurity principles for a holistic approach to threats; and 3. (End-User Aspect): End Users plan for and know how to respond to, withstand, operate through, and recover from PNT disruptions and interference, as well as understand and minimize the impact of PNT disruptions in downstream systems. In addition, the ICG members should consider the promotion of the principles of this recommendation to other UN member states, including the ICG WG C activities.

Members Consensus Reached _____ ; **No Consensus Reached** _____

Chairperson Signature: _____ **Date:** _____