MARINE CIRCULAR 06/2025 – GPS Spoofing and Enhancing Cybersecurity

Barbados Maritime
Ship Registry

Revision No:	1.0	Issue Date:	30/Jul/2025	Effective Date:	30/Jul/2025

Notice to: Shipowners, Operators, Masters, and all other parties concerned

1. Background

1.1 The Maritime Safety Committee, at its 104th session (4th to 8th October 2021), through MSC.1/Circ.1644, considered the deliberate interference with Global Navigation Satellite Systems (GNSS) and the United States' Global Positioning System (GPS), as reported in various locations throughout the world. The Committee recalled that satellite navigation system signals are vulnerable to deliberate interference intended to disable or deceive signal receivers and integrated navigational and communications equipment.

1.2 The Committee noted that these incidents of deliberate interference have been reported in several locations and were evaluated by certain organisations having specialised equipment and expertise necessary to analyse the cause and impacts to maritime shipping.

1.3 The Committee also noted that the deliberate interference with satellite navigation system signals possess a substantial risk to the safety of navigation, the safety of life and property, and the protection of the marine environment.

1.4 The Committee reminded Member States of their responsibility to refrain from interfering with GPS and GNSS signals.

2. Purpose

2.1 As of the current date, the International Maritime Organization (IMO) has not issued any specific guidelines solely for mitigating GPS spoofing on ships. However, the maritime industry acknowledges the significant threat posed by GNSS jamming and spoofing, which can disrupt critical positioning, navigation, and timing (PNT) data essential for maritime safety.

2.2 This Marine Circular provides for the issue of warning notices to minimise negative effects upon maritime operations as per MSC.1/Circ.1644 and for advice on best practices on mitigating GPS spoofing and enhancing cybersecurity in maritime operations.

2.3 By implementing these measures, maritime organisations can significantly enhance their cybersecurity posture and can better protect their operations from cyber threats.

2.4 Operators are advised to contact the vessel’s Recognised Organisation and the provider of the systems and services installed on board the vessel for better and more detailed action.

3. GNSS Jamming and Spoofing

3.1 To Address GNSS Jamming and Spoofing Threats:

.1 Monitoring and Detection:

i) Remain vigilant for position loss alarms and any unexpected deviations on the Electronic Chart Display and Information System (ECDIS);
ii) Regularly compare radar data with ECDIS to identify inconsistencies that could indicate spoofing.

.2 Response Procedures:

i) In case of confirmed GNSS disruptions, switch to Dead Reckoning mode;
ii) Commence manual position plotting, using all other available means, including radar and celestial observations, to maintain navigational accuracy;
iii) Implement enhanced monitoring using additional visual lookouts and radar-based navigation techniques to mitigate the risks of GNSS unreliability.

.3 Training and Awareness:

i) Ensure crew members are trained to recognise signs of GNSS spoofing and understand appropriate response protocols;
ii) Incorporate GNSS disruption scenarios into regular safety drills and training programs.

.4 Technological Measures:

i) Consider investing in anti-jamming and anti-spoofing technologies to enhance the resilience of navigation systems against such threats;
ii) By integrating these measures into standard operating procedures, shipping companies can better safeguard their vessels against the risks associated with GPS spoofing.

4. Enhancing Cybersecurity

4.1 For Enhancing Cybersecurity in Maritime Operations:

.1 Risk Assessment and Management:

i) Conduct regular risk assessments to identify potential vulnerabilities and areas needing improvement;
ii) Develop a comprehensive cybersecurity risk management plan tailored to specific maritime operations.

.2 Access Control:

i) Implement strict access control measures to ensure only authorised personnel can access sensitive systems and data;
ii) Use multi-factor authentication and robust password policies to enhance security.

.3 Network Security:

i) Segregate networks to limit the impact of potential breaches and prevent unauthorised access between different systems;
ii) Deploy firewalls, intrusion detection systems, and intrusion prevention systems to protect against external threats.

.4 Regular Software Updates and Patch Management:

i) Keep all software and systems up to date with the latest security patches and updates to protect against known vulnerabilities.

.5 Training and Awareness:

i) Conduct regular cybersecurity training for crew members and shore-based staff to raise awareness and educate them about potential threats and best practices;
ii) Develop a culture of cybersecurity awareness where everyone understands their role in maintaining security.

.6 Incident Response Planning:

i) Develop and regularly update an incident response plan to ensure a swift and effective response in the event of a cybersecurity incident;

ii) Conduct drills and simulations to test the effectiveness of response plans and improve preparedness.

.7 Data Encryption:

i) Use encryption to protect sensitive data both in transit and at rest, ensuring confidentiality and security.

.8 Physical Security:

i) Implement physical security measures to protect IT infrastructure and equipment from unauthorised access or tampering.

.9 Collaboration and Information Sharing:

i) Collaborate with industry partners, government agencies, and cybersecurity experts to share information about threats and best practices;

ii) Participate in cybersecurity initiatives and forums to stay informed about emerging threats and solutions.

.10 Compliance with Regulations and Standards:

i) Adhere to relevant international and national cybersecurity regulations and standards, such as the IMO's guidelines on maritime cybersecurity.

5. Useful Links

5.1 A list of useful links, although not exhaustive, is provided below for more information on the subject.

.1 https://britanniapandi.com/2024/10/navigational-risks-at-sea-the-growing-threat-of-gnss-jamming-and-spoofing/

.2 https://north-standard.com/insights-and-resources/resources/articles/gps-jamming-spoofing-and-hacking

.3 https://www.imo.org/en/mediacentre/pressbriefings/pages/joint-imo-icao-itu-statement-satellite-interference.aspx

.4 https://wwwcdn.imo.org/localresources/en/MediaCentre/PressBriefings/Documents/ICAO-IMO-ITU%20Joint%20Statement.pdf

6. Validity

6.1 The validity of this circular is until withdrawn or superseded.

For any inquiries or clarifications for this marine circular, please contact:

ops@barbadosmaritime.com
Operations Department
Barbados Maritime Ship Registry