U.S. MARITIME ADVISORY 2023-013
Threat Type: GPS Interference & AIS Spoofing
Geographic Area: Various

This advisory cancels U.S. Maritime Advisory 2023-005

1. Reference: None.

2. Issue: Instances of significant GPS interference have been reported worldwide in the maritime domain. This interference can result in lost or inaccurate GPS signals affecting bridge navigation, GPS-based timing, and communications equipment (including satellite communications equipment). The U.S. Coast Guard Navigation Center (NAVCEN) webpage, https://navcen.uscg.gov/gps-problem-report-status, contains a chronological list of recently reported GPS problems. GPS interference may also be caused by planned testing or training activities. Further information on planned outages can be found at https://www.navcen.uscg.gov/gps-service-interruptions, and will also be published in the Notice to Mariners.

Automatic Identification Systems (AIS) are open, unencrypted, and unprotected radio systems intended to operate on non-secure VHF-FM channels. As such, AIS signals can be spoofed, resulting in incorrect or missing AIS data.

3. Guidance: Exercise caution when underway. Plans for responding to GPS disruptions that affect safe navigation of vessels should be in place prior to getting underway. Such plans should be incorporated into company policy and safety management systems as appropriate and made readily available to vessel crew responsible for safe navigation of the vessel.

When a GPS outage occurs, incidents should be reported in real time. The NAVCEN and NATO Shipping Centre websites contain details on the reporting process for disruptions, requesting critical information such as the location (latitude/longitude), date, time, and duration of the outage/disruption. Additionally, providing photographs or screen shots of equipment failures experienced may facilitate analysis. The NAVCEN reporting information is available at: https://www.navcen.uscg.gov/report-a-problem. NATO Shipping Centre reporting information is available at https://shipping.nato.int/nsc/page10303037.

AIS devices do not always have virus or malware protection installed, so cyber security best practices against hacking should be adhered to if you connect your AIS to a network or update it using removable electronic devices (e.g. USB drives). AIS, while an invaluable situational tool, should never be solely relied upon for collision avoidance or navigational decision-making.

4. Contact Information: Maritime GPS disruptions or anomalies should be reported immediately to the NAVCEN at https://www.navcen.uscg.gov/report-a-problem or via phone at 703-313-

5900, 24-hours a day. NAVCEN will further disseminate reported instances of GPS interference to the NATO Shipping Centre.

Should you encounter ghost or fake AIS targets, please report them to the NAVCEN at https://www.navcen.uscg.gov/report-a-problem .

5. Cancellation: This message will automatically expire on March 30, 2024.

For more information about U.S. Maritime Alerts and Advisories, including subscription details, please visit https://www.maritime.dot.gov/msci.