U.S. MARITIME ADVISORY 2023-005
Threat Type: GPS Interference & AIS Spoofing
Geographic Area: Various

This advisory cancels and updates U.S. Maritime Advisory 2022-010

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). Over the last six months, an area in which multiple instances were reported was the Strait of Hormuz. 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.

Additionally, 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 and prior to getting underway. The NAVCEN and NATO Shipping Center websites contain information regarding effective navigation practices for vessels experiencing GPS interference. The information reaffirms safe navigation practices when experiencing GPS interference, provides useful details on reporting disruptions, and is intended to generate further discussion within the maritime community about other disruption mitigation practices and procedures. This guidance also recommends reporting such incidents in real time; noting critical information such as the location (latitude/longitude), date, time, and duration of the outage/disruption; and providing photographs or screen shots of equipment failures experienced to facilitate analysis. The NAVCEN information is available at: https://mariners.coastguard.blog/2017/09/21/9212017-good-navigation-practices-how-one-vessel-master-managed-safe-navigation-during-a-gps-outage/. NATO Shipping Center information is available at https://shipping.nato.int/nsc/page10303037.

AIS devices do not inherently have virus or malware protection, 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 Center.

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 September 4, 2023.

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