Billing Code 4910-9X

DEPARTMENT OF TRANSPORTATION

Workshop on GPS Jamming and Spoofing in the Maritime Environment

[DOT-OST-2020-0237]

AGENCY: Office of the Assistant Secretary of Transportation for Research and Technology (OST-R), U.S. Department of Transportation (DOT).

ACTION: Notice of public meeting.

SUMMARY: The purpose of this notice is to inform the public that DOT, through the Office of the Assistant Secretary for Research and Technology (OST-R) and the Maritime Administration (MARAD), will host a workshop on Global Positioning System (GPS) jamming and spoofing in the maritime environment on December 3, 2020. The workshop will focus on:

- How positioning, navigation, and timing (PNT) supports maritime applications;
- What happens when PNT is denied, disrupted, or manipulated in a maritime environment; and
- Options to reduce operational impact and increase PNT resiliency.

This DOT Workshop will be held virtually and is open to the general public by registration only. For those who would like to attend the workshop, we request that you register no later than November 30, 2020. Please use the following link to register: https://volpe-events.webex.com/volpe-events/onstage/g.php?MTID=e8d794472bbf3089c77da9ac1c31efdc2

You must include:

- Name
- Organization
- Telephone number
- Mailing and e-mail addresses

- Country of citizenship

Several days before the workshop, an email containing the agenda, dial-in number, and WebEx information will be provided. DOT is committed to providing equal access to this workshop for all participants. If you need alternative formats or services because of a disability, please contact Elliott Baskerville (contact information listed below) with your request by the close of business on November 27, 2020.

DATE AND TIME: December 3, 2020, from 1:00-5:00 PM (EST).

LOCATION: This workshop will be held virtually.

FOR FURTHER INFORMATION CONTACT: Elliott Baskerville, Office of Positioning, Navigation, and Timing & Spectrum Management, Office of the Assistant Secretary for Research and Technology, U.S. Department of Transportation, 1200 New Jersey Ave. SE, Washington, DC 20590, 202-366-5284, Elliott.Baskerville@dot.gov.

SUPPLEMENTARY INFORMATION:

1. Overview

Accurate and reliable PNT capabilities are essential for the safety for all modes of transportation and will become increasingly important for automated vessels. The primary and most recognizable PNT service supporting critical infrastructure is GPS. However, because GPS relies on signals broadcast from the satellite constellation, its signals are low power at the receiver and are thus vulnerable to intentional and unintentional disruption, such as jamming and spoofing. GPS "jamming" involves the use of a device to block or interfere with GPS signals; "spoofing" is deceiving a GPS device through fake signals. Both phenomena undermine the reliability of GPS and may have adverse consequences for maritime safety and commerce.

Jamming has long been a threat to GPS due to the weak signal power from the GPS satellites. North Atlantic Treaty Organization (NATO) military drills in the Baltic Sea last year, with 40,000 troops and all 29 Nations participating, experienced GPS jamming. Spoofing was considered an unrealistic threat for many years because it is complicated to perform. However, high-profile demonstrations at the University of Texas that spoofed a drone and a sophisticated yacht brought spoofing into the public eye in 2012-2013, a little more than a decade after DOT's Volpe National Transportation Systems Center (Volpe Center) issued its report, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System" (August 2001; available at: https://rosap.ntl.bts.gov/view/dot/8435).

A likely GPS spoofing attack occurred in the Black Sea in 2017, where over 20 ships erroneously reported their GPS positions as being inland at an airport. The number of separate vessels that reported the same false position and the characteristic jumping between the false and true position of the ships is strong evidence of a large-scale spoofing attack. More recently, incidents of GPS spoofing have been occurring around the world, particularly in maritime environments. The U.S. Government provides advisories of GPS interference through the Maritime Security Communications with Industry (MSCI) portal, at https://www.maritime.dot.gov/msci/2020-016-various-gps-interference.

Much of global trade is conducted by waterways, where ports are often congested and visibility is variable. In a maritime environment, GPS not only provides positioning information, but also provides inputs to speed, heading, steering, radar and target information, Electronic Chart Display Information System (ECDIS), Under Keel Clearance (UKC), and the Automatic Identification System (AIS). Being able to detect when spoofing is occurring is vital, since over 50% of all casualties at sea occur due to navigation issues. When GPS jamming and spoofing is

detected, the goal is for ships to immediately switch to other navigation tools. It is therefore critical to use complementary PNT technologies to ensure PNT resiliency.

Consistent with these concerns, on February 12, 2020, President Trump issued Executive Order (EO) 13905, *Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services*. The goal is to foster the responsible use of PNT services by critical infrastructure owners and operators (including the transportation sector) to strengthen national resilience. EO 13905 seeks to ensure that disruption or manipulation of PNT services does not undermine the reliability or efficiency of critical infrastructure by:

- Raising awareness of the extent to which critical infrastructure depends on PNT services;
- Ensuring that critical infrastructure can withstand disruption or manipulation of PNT services; and
- Engaging the public and private sectors to promote responsible use of PNT services.

In accordance with Section 4(g) of EO 13905, DOT is conducting a pilot program to inform the development of the relevant PNT profile and research and development (R&D) opportunities. The DOT pilot program, led by OST-R and MARAD, is focused on addressing GPS jamming and spoofing impacts to maritime vessels through stakeholder engagement and evaluating complementary PNT technologies that can be adopted to mitigate the impacts during these threat scenarios. The DOT pilot program will be conducted through stakeholder engagement and evaluation of complementary PNT technologies that can be adopted to mitigate the impacts during these threat scenarios.

The purpose of the workshop, which is a key component of stakeholder engagement of the DOT pilot program, is to increase public awareness of real-world incidents of the GPS signal being jammed or spoofed in a maritime environment and to discuss potential options to detect this

interference, as well as use of complementary PNT technologies to provide a resilient PNT capability in the maritime environment.

Issued This 20th Day of November, 2020 in Washington, DC.

Diana Furchtgott-Roth,

Deputy Assistant Secretary for Research and Technology,

U.S. Department of Transportation.

[FR Doc. 2020-26120 Filed: 11/24/2020 8:45 am; Publication Date: 11/25/2020]