



## Orolia to Host Second Industry Discussion on PNT Executive Order

*Vulnerability Testing to Protect Critical Infrastructure*

**Rochester, NY- June 24, 2020** - Orolia will host a second industry discussion on the [Positioning, Navigation and Timing \(PNT\) Executive Order](#), a federal initiative to protect critical infrastructure from GPS/GNSS jamming and spoofing threats, and other PNT service disruptions.

This session will explore the importance of vulnerability testing to protect critical infrastructure with Resilient PNT technologies. The defense industry has addressed complex GNSS and PNT threats longer than any other sector, and experts will share their insights and best practices to help inform the protection strategy for critical infrastructure identified in the Executive Order.

Vulnerability testing with GNSS simulation is essential to protect critical infrastructure. However, there is no one size fits all approach. This testing requires the ability to customize scenarios per application. It also needs to identify gaps across a variety of unique and geographically distributed systems. Test results provide the basis to select the best PNT technologies to increase resilience, while ongoing regular testing ensures that critical systems can adapt and overcome evolving threats.

The Orolia PNT Coffee Talk™ is for those interested in learning more and discussing the latest developments in this national priority from industry and government perspectives.

**What:** PNT Coffee Talk- Vulnerability Testing for Critical Infrastructure:  
Lessons Learned from Defense

**When:** July 16, 2020 at 2 pm EST

**Where:** Online- [register here](#)

### **About GPS Jamming and Spoofing**

*GPS Jamming* disrupts or denies access to signals and the PNT data that they transmit. When those signals and data are manipulated, that is *Spoofing*, and it is often more dangerous. During spoofing attacks, the target does not know that they are under attack and they continue to rely on compromised data.

These global threats are increasing and becoming more sophisticated, with many documented attacks reported worldwide. They can deny access to, or compromise, essential PNT data in sectors such as defense, homeland security, transportation, power grids, communications/mobile, precision agriculture, weather forecasting and emergency response. Learn more in Orolia's [Jamming and Spoofing Resource Center](#).

### **About Orolia**

Orolia is the world leader in Resilient Positioning, Navigation and Timing (PNT) solutions, even in GPS denied environments. With a presence in more than 100 countries, Orolia provides virtually fail-safe GPS/GNSS and PNT solutions for military and commercial applications worldwide. [www.orolia.com](http://www.orolia.com)

### **Press Contact:**

Jennifer Hewitt

(571) 388-8671

[jennifer.hewitt@orolia.com](mailto:jennifer.hewitt@orolia.com)

###