

THE ROLE OF PNT IN CRITICAL INFRASTRUCTURE

Accurate position, navigation, and timing (PNT) is necessary for the functioning of many critical infrastructure sectors. Precision timing is one aspect that is particularly important, with one microsecond level or better synchronization often being required by numerous infrastructure systems, such as the electric grid, communication networks and financial institutions. Currently, the primary source of distributed and accurate timing information is through the Global Positioning System (GPS). However, GPS' space-based signals are low power and unencrypted, making them susceptible to both intentional and unintentional disruption.

To address GPS vulnerabilities in critical infrastructure, this program focuses on four areas:

- Vulnerability and Impact Assessment
- Mitigations
- Outreach and Education
- Diversifying Timing Technologies

VULNERABILITY AND IMPACT ASSESSMENT

To better understand vulnerabilities at the end-user equipment level, testing and evaluation is being conducted on an array of commercial GPS receivers used within the critical infrastructure sectors. This will help characterize the GPS receivers' behavior under various scenarios and identify key vulnerabilities.

Analysis is also being performed to better understand the national impacts and consequences of timing disruptions to critical infrastructure. These system-level risk and impact assessments will help prioritize mitigation efforts.

MITIGATIONS

Mitigations range from implementing best practices to developing improved, more secure hardware. Examples include improving situational awareness by developing the capability to detect and automatically alert users of jamming or spoofing events, working with equipment manufacturers to ensure newer product lines are more robust to existing threats, and developing new antenna designs optimized to minimize jamming and spoofing effects on GPS receivers.

OUTREACH AND ENGAGEMENT

A key element of this program is outreach to stake-holders to educate them on threats, vulnerabilities, impacts, and mitigations. Equipment manufacturers and critical infrastructure owners and operators are a crucial part of this effort. DHS S&T is leading an industry working group to develop a conformance framework that defines levels of security and resilience for timing equipment.



Most critical infrastructure sectors rely heavily on GPS to provide position, navigation, and timing information.

DIVERSIFYING TIMING TECHNOLOGIES

In addition to mitigation capabilities, DHS S&T is assessing complementary timing technologies to reduce reliance on a single system (i.e. GPS). This effort is driven by National Security Presidential Directive-39 (NSPD-39) of 2004.

Alternative timing technologies will not only provide new sources of robust timing data, but they will also hamper jamming and spoofing attempts, as having complementary timing sources enables comparison and validation of timing data.

THE FUTURE OF RESILIENT PNT

Executive Order 13905, Strengthening National Resilience through Responsible Use of PNT Services, promotes the responsible use of PNT services by the federal government and critical infrastructure owners and operators. DHS S&T and Cybersecurity and Infrastructure Security Agency (CISA) will strive to make PNT an integral part of the overall risk analysis process.