



IT Security



Supply Chain



OT Security



Insider Threat



Physical Security



Interoperable Communications

# CISA INSIGHTS



## GLOBAL POSITIONING SYSTEM (GPS) INTERFERENCE

*December 2022*

The Cybersecurity and Infrastructure Security Agency (CISA) has been working with government and industry partners to increase resilience to GPS disruptions that could impact critical infrastructure operations. The national Position, Navigation and Timing (PNT) ecosystem heavily relies on GPS as the primary source of position navigation and timing. The event below illustrates how PNT users should understand the impacts to operations should GPS be unavailable.

### EVENT SUMMARY

In January 2022, a GPS interference event occurred over a thirty-three (33) hour period in the vicinity of Denver International Airport due to a transmitter errantly broadcasting in the GPS frequency. Interference was first detected by aircraft pilots and communicated to Federal Aviation Administration (FAA) Air Traffic Control Facilities. Due to the significant number of reports, the FAA issued a Notice to Air Missions warning of the GPS interference.

Operators of systems from a wide range of critical infrastructure that rely on the GPS signal for uninterrupted PNT services also detected interference with (1) surface and rail traffic and (2) communications towers and services using GPS timing signals. Ground-based industry users of GPS/PNT services and others reported GPS interference to the United States Coast Guard Navigation Center (NAVCEN) and the Federal Communications Commission (FCC) Public Safety and Homeland Security Bureau.

Departments and agencies responsible for monitoring and coordinating response to GPS interference events implemented the established national coordination process. The FCC Enforcement Bureau deployed, located, and coordinated shut down of the emitter. No accidents or injuries occurred because of the GPS interference incident. However, several critical infrastructure sectors were degraded. Many systems that detected the event had resilient alternate timing built in for backup or fail-over timing and experienced minor or no degradation of services.

An investigation of the interference positively identified an emitter unintentionally transmitting a signal within the GPS L1 frequency. Some receivers within a line of sight of the transmitter experienced GPS signal disruption. The affected area on the ground covered approximately 50 nautical mile radius on the ground and spanned approximately 230 nautical miles in distance from the interfering transmitter at flight levels up to approximately 36,000 feet.

Improving interference detection and mitigation (IDM) of GPS signal interference is a priority of CISA. CISA is leading a federal government interagency after-action review of the event to (1) encourage owner/operator resilience by sharing best practices, (2) improve capabilities, processes, and procedures on reporting GPS interference and (3) encourage shared situational awareness with the goal of enhancing government and industry information sharing to further improve expediting IDM of interfering emissions, affecting GPS signals over the United States and its territories.

## WHAT IS GPS AND HOW DOES IT WORK?

GPS is an extremely reliable space-based PNT service provided without direct cost to the public and has become increasingly important to a wide range of critical infrastructures. The GPS satellite constellation provides a signal from satellites in orbit around the Earth, managed by the control segment, to be used by the user segment. These signals are very weak at ground level and can be easily overpowered by unwanted transmissions.

Critical Infrastructure operations that leverage GPS include:

- Position and navigation for marine, terrestrial and aviation services,
- Communications network operations,
- Timing supporting for the power sector, and other critical infrastructure industrial control systems,
- Time stamping banking and financial services transactions, and
- A wide range of secondary dependencies, especially in computer and internet network operations.

## WHAT CAN CAUSE GPS INTERFERENCE AND HOW IS IT DETECTED?

GPS signal interference can be caused by malfunctioning or incorrectly configured transmitters, which can inadvertently broadcast signals in the same frequency range as GPS transmissions. GPS interference can also be intentional, when jamming devices emit signals in the GPS frequency. Some transportation organizations use GPS tracking devices to track speed and location of their asset. As identified by NBC News and documented in FCC enforcement actions, GPS jammers are being deployed on vehicles where the vehicle operator is jamming the signal to undermine the company's fleet use policies<sup>i</sup>.<sup>ii</sup> Intentional interference is a violation of law enforced by the FCC<sup>iii</sup>.

Detecting interference can be challenging. GPS signals can be blocked by objects or moving inside of buildings. If user equipment is in good operating condition and normally has a good GPS signal in a specific area, on a roadway, or clear line of sight to satellites and loses signal reception, there is a good chance that there is signal interference.

The GPS constellation is extremely reliable and multiple receivers should not lose reception at the same time. Critical infrastructure owners with systems which rely on GPS services commonly monitor logs to ensure GPS signal availability and have system alarms when there is GPS signal disruption. If logs and alarms show GPS is unavailable over several receivers of different makes and models, there may be GPS signal interference, especially if the GPS signal is lost on multiple systems simultaneously, such as industrial networks and personal cell phones at the same general location. However, GPS signal interference is a complex issue. Users should work with their equipment providers to understand the steps needed to determine if there is an equipment malfunction and establish predefined troubleshooting procedures. Working with equipment providers, users could identify alternate timing sources or extended holdover capabilities that may assist continued timing operations during GPS interference events. When in doubt, users should report suspected GPS signal interference.

## WHEN AND HOW DO I REPORT GPS SIGNAL INTERFERENCE?

GPS signal interference should be reported anytime it is believed there is an outage. GPS signal interference that extends for hours or affects multiple receivers is a low occurrence event. Timely reporting to the appropriate Operations Center is important to properly attribute the source of interference, even when GPS users are resilient and have successfully continued operating using an alternate timing source (such as an atomic clock).

## Pilots Experiencing

### a GPS Anomaly

Pilots experiencing a GPS anomaly should report the time, location, speed, magnetic heading altitude, and duration of the outage.

Pilots in-flight immediately report, by radio contact, to the controlling Air Traffic Control (ATC) facility or Flight Service Station (FSS) and, by telephone, to the nearest ATC facility controlling the airspace where the disruption was experienced.

Additionally, post-flight, pilots should complete the GPS Anomaly Reporting Form located on the Federal Aviation Administration (FAA) website at: [www.faa.gov/air\\_traffic/nas/gps\\_reports/](http://www.faa.gov/air_traffic/nas/gps_reports/).

*These operations centers (FAA, NAVCEN and FCC) closely coordinate to rapidly analyze, investigate, and attribute the source of interference and response to and recover from GPS interference events.*

### Maritime or Terrestrial Users Experiencing a GPS Anomaly

Maritime or terrestrial users experiencing GPS signal interference should report via the U.S. Coast Guard's Navigation Center (NAVCEN) website [www.navcen.uscg.gov/report-a-problem](http://www.navcen.uscg.gov/report-a-problem) or via phone at 703-313-5900.

Additionally, if the jamming or interference is presenting an imminent life-threatening problem, contact the FCC's 24/7 Operations Center at 202-418-1122 or [FCCOPS@fcc.gov](mailto:FCCOPS@fcc.gov). Complaints of Radio Frequency interference can be filed at FCC's Public Safety Radio Frequency Service Interference Complaint Portal: <https://fccprod.servicenow.com/psix-esix>.

## RESOURCES

The Department of Homeland Security (DHS) has been working on the issue of GPS interference for many years. DHS's Science & Technology Directorate in coordination with the CISA and the National Coordination Office for Space-Based Positioning, Navigation and Timing published best practices for installing equipment that is better able to accommodate imperfections in their inputs, regardless of whether these imperfections are intentional or not. These best practices provide owners, operators, researchers, designers, and manufacturers with information to improve the security and resilience of PNT equipment across the spectrum of equipment development, deployment, and use.

- Best Practices Guide: [Improving the Operation and Development of Global Positioning System \(GPS\) Equipment Used by Critical Infrastructure \(cisa.gov\)](#)
- CISA PNT Webpage: [CISA.gov/pnt](http://CISA.gov/pnt)
- DHS Science & Technology Directorate's PNT Program: [DHS.gov/science-and-technology/pnt-program](http://DHS.gov/science-and-technology/pnt-program)
- United States Coast Guard's NAVCEN Webpage: [www.navcen.uscg.gov/](http://www.navcen.uscg.gov/)
- GPS – The Global Positioning System Webpage: <https://www.gps.gov/>

<sup>i</sup> <https://www.nbcnews.com/news/us-news/gps-under-attack-crooks-rogue-workers-wage-electronic-war-n618761>

<sup>ii</sup> Search Results | Federal Communications Commission (fcc.gov)

<sup>iii</sup> [Jammer Enforcement | Federal Communications Commission \(fcc.gov\)](#)