U.S. Space-Based Positioning, Navigation and Timing (PNT)

60th Meeting of the Civil GPS Service Interface Committee

22 September 2020

Harold W. Martin III
Director
National Coordination Office
Opposition to FCC Ruling on Ligado

• On April 20, 2020, the Federal Communications Commission (FCC) announced that, "it has approved with conditions Ligado's application to deploy "a low-power terrestrial nationwide network in the L-Band that will primarily support 5G and Internet of Things services."

• The Executive Branch (which is separate from FCC) is concerned because Ligado's proposed transmission power exceeds the thresholds established by the GPS Adjacent Band Compatibility study to protect GPS users from harmful interference.
On December 6, 2019, the National Telecommunications and Information Administration (NTIA) released a letter on behalf of the National Executive Committee for Space-Based Positioning, Navigation, and Timing (PNT EXCOM) to the Federal Communications Commission (FCC) transmitting the executive branch's position on a spectrum plan proposed by Ligado Networks.

- "The PNT EXCOM is charged with the responsibility to advise and make recommendations to its member Departments and Agencies that ensure services provided by U.S. space-based PNT infrastructure, including the GPS constellation and GPS augmentations, are made available consistent with the U.S. Space-Based PNT Policy in support of U.S. national security, homeland security, foreign policy, economic, public safety, and scientific interests."

- "With regard to the license modification application of Ligado Networks to the Federal Communications Commission, it is clear that the proposed service would exceed the tolerable power limits necessary to prevent disruption of GPS receivers. Based on the results of the extensive studies the NTIA should recommend to the FCC against approval of the license modification."

The full letter can be found at GPS.gov
Opposition to FCC Ruling on Ligado

The Defense Department opposes a license the Federal Communications Commission has granted to a private company, Ligado, to deploy a low-power nationwide mobile broadband network. Here's why:

- **GPS disruptions caused by Ligado interference could have global ramifications to U.S. national security, commercial and civil sectors, the economy, and those who rely on this service in their everyday lives.**
- **There are too many unknowns, and the risks are too great, to allow the proposed Ligado system to proceed. We risk lives and the security of the nation if GPS is interrupted for any amount of time.**
- **There is no need to put GPS at risk. Mid-band spectrum for 5G exists, and DOD is working with industry on a dynamic spectrum sharing framework. Ligado's proposal is unnecessary.**
- **Ligado's proposed network lacks the bandwidth, power or global ecosystem to deliver robust 5G services. The only beneficiaries are Ligado shareholders.**

"The Global Positioning System signal and service need to be protected based on the importance of GPS to national security, civil services and the economic benefits to the nation."

— Defense Secretary Dr. Mark T. Esper
DOT opposed the FCC decision to allow Ligado to deploy a nation-wide mobile broadband network and has multiple concerns:

**Summary of DOT Concerns**

- The DOT GPS Adjacent Band Compatibility (ABC) test results clearly demonstrate there will be widespread disruption to GPS receivers.

- DOT serves as the Civil Lead for GPS and is concerned about the millions of receivers that will experience interference:
  - The majority of civil GPS receivers are not U.S. Government devices and will not qualify for repair or replacement paid for by Ligado.

- FCC should thoroughly assess and account for the economic costs and burdens that will result:
  - Many GPS/GNSS receivers are hermetically sealed so it is not possible to retrofit them with new antennas.
  - Furthermore, many receivers are integrated into end-user applications making adversely affected GPS users unable to retrofit or replace their GPS receivers.
Opposition to FCC Ruling on Ligado

Statement from the Department of Homeland Security on Ligado

Release Date: April 21, 2020

“The Department of Homeland Security recommended the FCC deny the Ligado license and remains concerned that an approval creates a high degree of uncertainty for our public and private sector partners, many of whom—along with the Departments of Homeland Security, Defense and Transportation, rely on precise and uninterrupted Positioning, Navigation and Timing (PNT) data from the Global Positioning System (GPS) to ensure the security and resilience of their infrastructure. Our critical infrastructure partners across the public and private sectors have similar dependence on PNT and GPS for the security and resilience of their operations.

If the FCC moves forward with its proposed action on Ligado, we will work with our partners to ensure procedures are in place to identify interference with GPS and rapidly implement mitigation measures while supporting the domestic deployment of 5G.

DHS will continue to work to manage risk to GPS receivers and promote the responsible use of PNT, in accordance with the President’s Executive Order.”
On behalf of the Executive Branch, the NTIA petitioned the Federal Communications Commission (FCC):

- The petition asks the FCC to rescind the grant, or to reconsider and modify the conditions it imposed on the grant in a number of critical respects. NTIA also petitioned the FCC to stay the effective date of the Order and Authorization while it considers NTIA’s reconsideration request.

- NTIA previously transmitted filings on behalf of the Executive Branch in December 2019 and April 2020 opposing the applications filed by Ligado to modify its licenses.

You can find the documents on GPS.gov
The U.S. must maintain its leadership in the service, provision, and use of Global Navigation Satellite Systems (GNSS)

- Continuous, worldwide, free of direct user fees
- Encourage compatibility and interoperability with foreign GNSS services and promote transparency in civil service provisioning
- Operate and maintain constellation to satisfy civil and national security needs
  - Foreign PNT services may be used to augment and strengthen the resiliency of GPS
- Invest in domestic capabilities and support international activities to detect, mitigate and increase resiliency to harmful interference
U.S. Policy

• NSPD-39, the Space-Based Positioning, Navigation, and Timing Policy from 2004, is in the process of being updated

• Space Policy Directive–X is currently in draft by the White House
Section 1606 requires, during FY 2018, the Secretary of Defense, the Secretary of Transportation, and the Secretary of Homeland Security to jointly develop a plan for carrying out a backup GPS capability demonstration for the Global Positioning System.

This section further states that, subject to the availability of appropriations, the Secretaries are required to jointly initiate the backup GPS capability demonstration and the Secretaries are required to submit a report on the demonstration.
On February 12, 2020, the President signed an Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services.

The order seeks to strengthen national resilience by identifying and promoting the responsible use of PNT services by the Federal Government and critical infrastructure owners and operators.

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. The national and economic security of the United States depends on the reliable and efficient functioning of critical
The Airwaves Are Not Safe

• Computers and the Internet: Once Upon a Time...
  • A GPS receiver is more computer than radio...
• GPS relies on spectrum – no longer a safe haven
• 900 Million U.S. GPS enabled devices require Cybersecurity
• U.S. Policy directs PNT resiliency (NSPD-39, PPD-4, PPD-21, EO 13800, National Cyber Strategy)
• SPD-5, Cybersecurity Principles for Space Systems is issued Sept 4, 2020

“Known but unmitigated vulnerabilities are among the highest cybersecurity risks...”
(EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)
What Can You Do Now?

• CIOs: Include GPS enabled devices in Cybersecurity plans

• Be a demanding customer - toughen GPS devices:
  • Incorporate valid range checking and other elements of latest GPS Interface Specification (IS-GPS-200K *)
  • Incorporate DHS Best Practices (Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure, Jan 2017 *)

* Documents available on www.gps.gov

Protect GPS and Critical Infrastructure that Relies on GPS
Thank You

Stay in touch: www.gps.gov

Contact Information:
National Coordination Office for Space-Based PNT
1401 Constitution Ave, NW – Room 62028
Washington, DC 20230
Phone: (202) 482-5809
www.gps.gov

GPS: Accessible, Accurate, Interoperable