GPS Interference Detection & Mitigation

National GNSS Research Center Workshop

Daejeon, KOREA

08 April 2011

Jeffrey Auerbach
GNSS Policy Advisor
Office of Space and Advanced Technology
U.S. Department of State
Overview

• LightSquared and potential GPS Interference

• U.S. Spectrum Management Process

• Interference Detection and Mitigation
  – Planned “Patriot Watch” Program
Existing/Emerging Global Threats

Links between Criminal & Terrorist activity are indisputable

GPS and GSM Jammer

U.K. £150

1 Watt Jammer

WA Post Aug 08

Police Turn to Secret Weapon: GPS Device

Aug 08, FCC cites Colorado business for selling GPS jammers to counter GPS vehicle trackers

NGRC Workshop, Daejeon, KOREA – 08 April 2011
LightSquared & GPS

• Plans to provide a nationwide wireless broadband network integrated with satellite coverage
  – Combine existing mobile satellite communications services with a ground-based wireless communications network that uses the same L-band radio spectrum as the satellites
  – Network will transmit signals in a radio band immediately adjacent to the GPS frequencies (1525-1559 MHz/1626.5-1660.5 MHz band)
  – Concern that ground-based transmissions may interfere with GPS signal

• 18 November 2010 - Request submitted to FCC for modification of its (ancillary terrestrial component) ATC authority

• 26 January 2011 - FCC Order & Authorization
  – Conditional approval to build out its ground-based wireless network
  – Requires addressing GPS concerns
• FCC required that LightSquared create a working group with the GPS community to address interference concerns
  – Final report to be submitted by 15 June 2011
  – Process must be completed to the Commission’s satisfaction before commencement of commercial service

• U.S. Government's National Space-Based PNT Systems Engineering Forum (NPEF) is conducting its own testing of the potential interference to GPS from the terrestrial network

www.pnt.gov/interference/lightsquared/
In the United States, responsibility for spectrum management including frequency allocations is divided between Federal Government uses and other uses.

The National Telecommunications and Information Administration (NTIA) is responsible for Federal Government uses, while the Federal Communications Commission (FCC) is responsible for all other uses.

Where responsibilities overlap, the FCC and NTIA reach a consensus through coordination.
National Spectrum Management

COMMUNICATIONS ACT OF 1934

THE PRESIDENT

NTIA

Federal Users
National Defense
Law Enforce & Security
Transportation
Resource Mgmt. &
Control
Emergencies
Space
Science/Research
Other Services

FCC
Non-Federal Users
Business
State & Local
Government
Entertainment
Commercial
Private

THE CONGRESS

COORDINATION

INTERDEPARTMENT RADIO ADVISORY COMMITTEE (IRAC)
Chaired by NTIA
20 Federal Agencies Represented
Regulations in the U.S.

• U.S. Federal statutes and regulations generally prohibit the manufacture, importation, sale, advertisement, or shipment of devices, such as jammers, that fail to comply with FCC regulations.

• U.S. Federal Statutes – Communications Act
  – 47 U.S.C. § 301 Unlicensed (unauthorized) operation prohibited
  – 47 U.S.C. § 333 – Willful or malicious interference to authorized communications prohibited
  – 47 U.S.C. § 302a(b) Manufacturing, importing, selling, offer for sale, shipment or use of devices which do not comply with regulations are prohibited
Regulations in the U.S.

• **Telecom Agency Rules - FCC**
  
  – 47 C.F.R. § 2.803(a) - marketing is prohibited unless devices are authorized and comply with all applicable administrative, technical, labeling and identification requirements.

  – 47 C.F.R. § 2.803(e)(4) - marketing is defined as “sale or lease, or offering for sale or lease, including advertising for sale or lease, or importation, shipment, or distribution for the purpose of selling or leasing or offering for sale or lease.”
FCC Education Campaign

www.fcc.gov/eb/jammerenforcement/
The United States Government shall:

- Protect global access to the radiofrequency spectrum required to support the use of space by the United States Government, its allies, and U.S. commercial users
- Address requirements for radiofrequency spectrum in the acquisition of space capabilities
- Ensure necessary regulatory frameworks remain in place over the lifetime of a system;
- Identify impacts to government space systems prior to reallocating spectrum
- Enhance capabilities and techniques, in cooperation with civil, commercial, and foreign partners, to identify, locate, and attribute sources of radio frequency interference
- Take necessary measures to sustain the radiofrequency environment in which critical U.S. space systems operate

Invest in domestic capabilities and support international activities to detect, mitigate, and increase resiliency to harmful interference to GPS
Critical Infrastructure and Key Resources (CIKR) Sectors

- Agriculture and Food
- Banking and Finance
- Chemical

- Commercial Facilities
- Communications
- Critical Manufacturing

- Dams
- Defense Industrial Base
- Emergency Services

- Energy
- Government Facilities
- Healthcare and Public Health

- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste

- Postal and Shipping
- Transportation Systems
- Water
• **DATA**: Collect, analyze, store, & disseminate interference incidents from all reporting sources

• **TOOLS**: Coordinate U.S. domestic capabilities to identify, analyze, locate, attribute, & mitigate sources of interference to the GPS & its augmentations

• **ACTION**: Develop & maintain capabilities, procedures & techniques, & routinely exercise civil contingency responses to ensure continuity of operations in the event that access to GPS signal is disrupted or denied
Planned U.S. “Patriot Watch” System

- System-of-Systems, open architecture, multi-phased approach to provide near real-time situational awareness of GPS in order to detect EMI & suspect purposeful interference to protect the Nations 18 CIKR Sectors
  - Designed with government and commercial hardware/software
  - Persistent monitoring for situational awareness
  - Timely response to anomalies
  - Sensor placement based on PNT CIKR Criticality
  - Remains operational when GPS systems is “stressed”
“Patriot Watch” Concept

National capability to detect & mitigate GPS interference in the U.S.

Leverage technologies to rapidly detect and locate interference

Provide standard response process and protocols to notify of abnormality

Establish command & control authority to mitigate events

GPS Satellites

Monitoring Network

Control Center

Mitigating action

Users

Re-route traffic
Summary

• Concerns over potential GPS interference from LightSquared proposal are being studied

• Civil infrastructure use of GPS drives requirement to build a national IDM capability

• “Patriot Watch” will provide situational awareness for Homeland Security and Homeland Defense

• Collaboration has been and continues to be a key element on building a successful system