Agenda

• Governance
• Existing and Emerging Threats
• Critical Infrastructure Interdependencies
• Patriot Watch Architecture
• Public Outreach – Collaboration with other Agencies
• Conclusions
Interference Detection & Mitigation (IDM) per NSPD 39
Existing and Emerging Threats

1,978,000 hits on “GPS Jammer”
Critical Infrastructure

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
Patriot Watch™ Initiative

• Protect the Nation’s 18 Critical Infrastructure & Key Resource Sectors (CIKR)

• System-of-Systems, Open Architecture, Multi-Phased/Multi-Layered Approach

• Near Real-Time Situational Awareness of Position Navigation and Timing (PNT) Interference
  – Leverage Existing mature capabilities & focus on the data, less on system/device
  – Common Data Structure for Information Sharing
Patriot Watch™ Architecture

Monitoring & Collection
- FCC/FAA Receiver/Sensors
- FAA MINNOW
- UNITRAC

Processing
- JLOC Master Station

Analysis & Evaluation
- Analyst
- USER
- USER
- USER

Other Systems that use GPS that could provide near real-time data:
- DGPS, CORS, Cell Sites, Transport Companies

FAA PNTIP
- SETS and COTS Jammer Library
Toll-Booth Concept

- Integrated with Camera System
- Alert Enforcement Personnel to Jammer Presence
- Detect & Track Jammers Approaching Entry Point
- Multi-Lane Distinction
- UNITRAC Database Connection

FCC Jammer Enforcement

http://www.fcc.gov/encyclopedia/jammer-enforcement

***ALERT***

Federal law prohibits the operation, marketing, or sale of any type of jamming equipment, including devices that interfere with cellular and Personal Communication Services (PCS), police radar, Global Positioning Systems (GPS), and wireless networking services (Wi-Fi).

"Jamming devices create serious safety risks. In the coming weeks and months, we'll be intensifying our efforts through partnerships with law enforcement agencies to crack down on those who continue to violate the law. Through education, outreach, and aggressive enforcement, we're tackling this problem head on."

-- P. Michele Ellison, Chief, Enforcement Bureau

For more information: http://www.fcc.gov/encyclopedia/jammer-enforcement
If you see something...

Say Something™

• USCG Navigation Website:
  – http://www.navcen.uscg.gov/?pageName=gpsUserInput

• Federal Communication Commission website:
  – http://www.fcc.gov/complaints
  – For further info e-mail: jammerinfo@fcc.gov
Conclusion

- Government (Federal and civil) agencies collaborating to address PNT IDM
- The ability to share information in a timely manner key to successful PNT IDM
- Leverage existing mature technologies that use GPS and harvest near real-time data
- Collecting data to support formal analysis; trends on jammers
- COTS Jammer Library will provide initial fingerprint of devices encountered
THANK YOU

John.Merrill@hq.dhs.gov
(202) 447-3731 PNT PMO
(202) 731-9628 Mobile