

# **PATRIOT WATCH**

**INTERFERENCE DETECTION MITIGATION (IDM)**

**VIGILANCE**

**SAFEGUARDING AMERICA**

**DHS Position, Navigation & Timing (PNT)  
Program Management Office  
John Merrill – Program Manager**

**August 14, 2012**





# Existing and Emerging Threats



Apple Accessories Computers & Peripherals Cell Car Electronics Security & Surveillance Entertainment Health & Lifestyle Cameras & Photo Batteries & Chargers All Categories

Categories

- Security & Surveillance
- Jammers**
- Door Phones
- Surveillance Cameras
- DVR Cards & Systems
- Cell Phone Booster
- Baby Monitors
- Baby Safety & Health

### Cell Phone Signal Jammer | GPS Blocker

**AMAZING DEAL!**

## Portable Cell Phone GPS Jammer

Block all GPS GSM CDMA  
Up to 30 Feet Jamming Radius

~~US\$73.98~~

**50% Off**

**US\$ 36<sup>99</sup>**

Get Your Here

**WEEKLY DEAL**

### 1600MHz GPS Signal Jammer

- Special for GPS L1
- Coverage: 3 - 6 Meter

US\$35.99

**US\$ 25<sup>99</sup>**

SAVE \$10

Save Now!

Buy Cell Phone Jammer kits, take a look at EspoTV's range of signal jammers & blockers.

Four small images showing different models of signal jammers. The first shows a black jammer with a 'No GPS' symbol. The second shows a black jammer with a 'No GPS' symbol. The third shows a white jammer with a 'No GPS' symbol. The fourth shows a black jammer with a 'No GPS' symbol.

1,978,000 hits on “GPS Jammer”



# Critical Infrastructure Key Resource Sectors (CIKR)



[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](#)

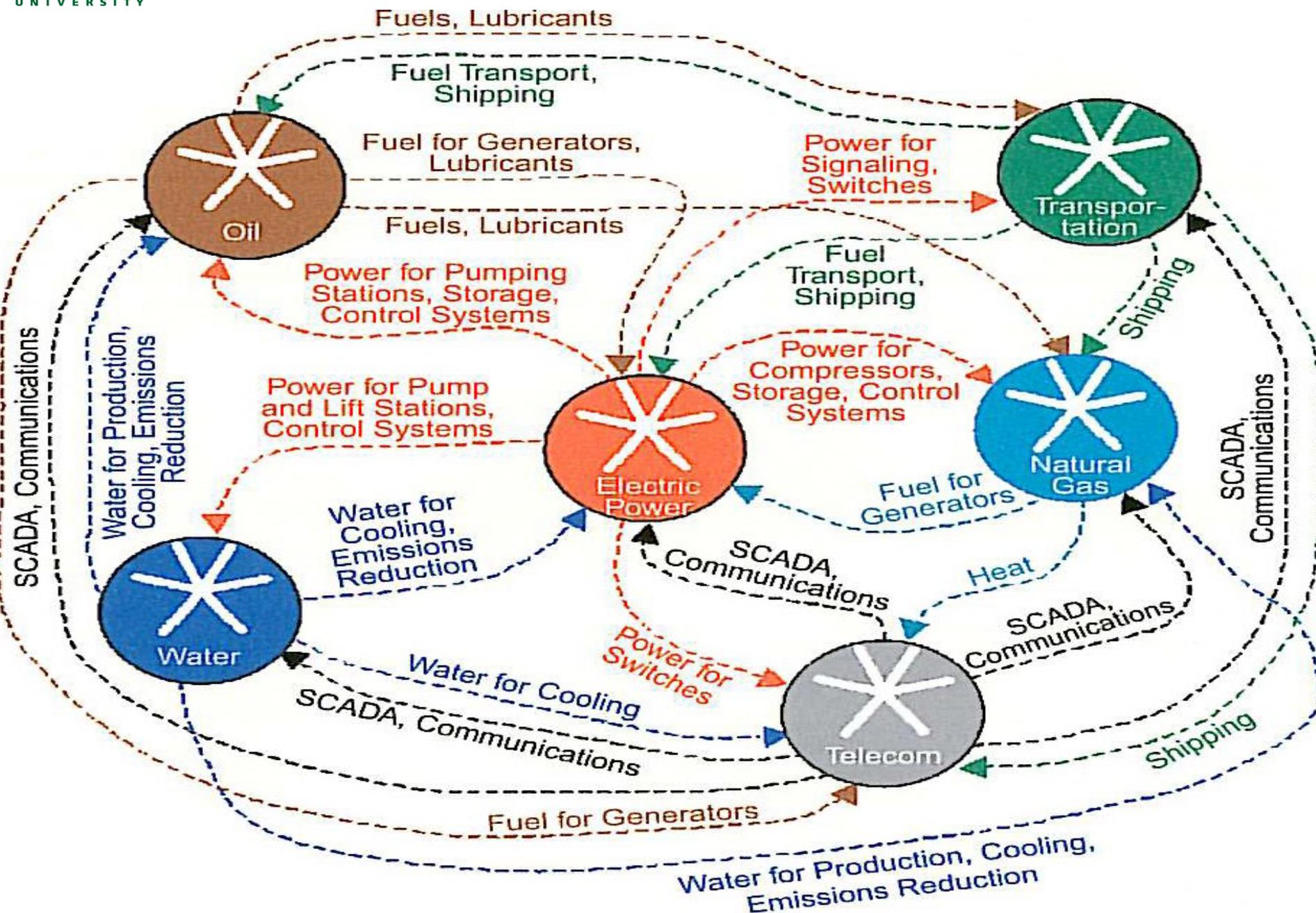


[Transportation Systems](#)



[Water](#)





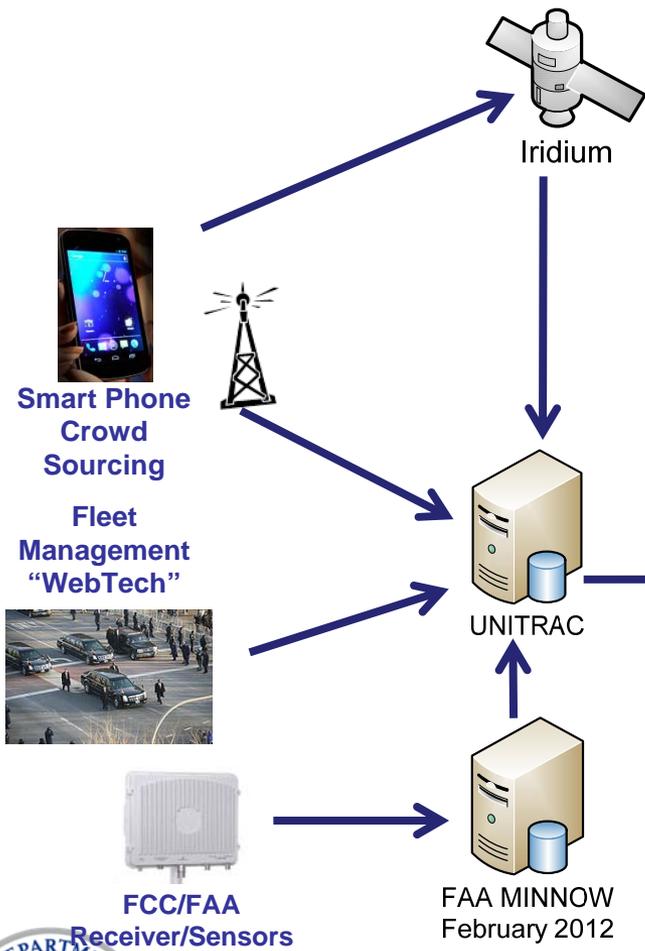
# Patriot Watch Initiative

- **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
  - Persistent Monitoring for Situational Awareness

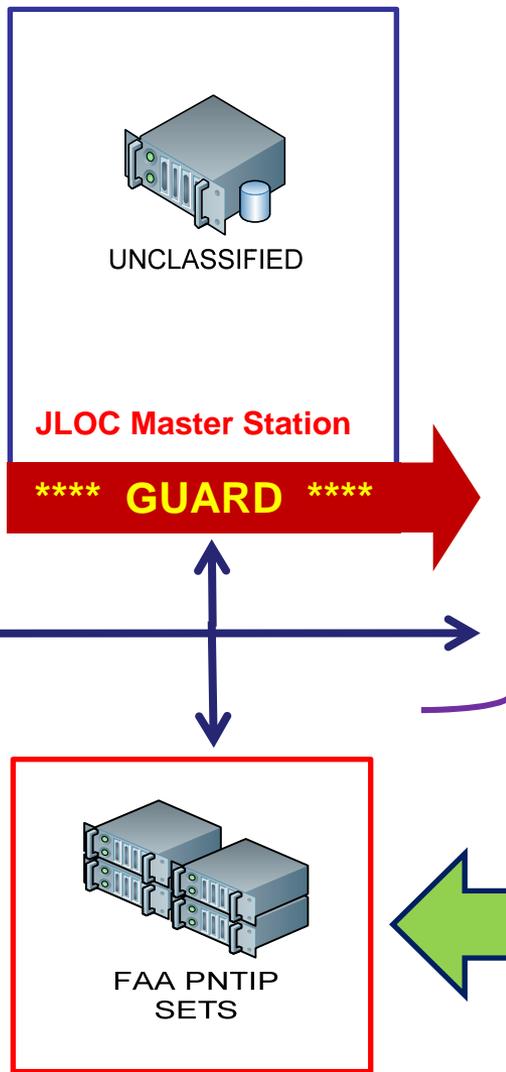


# Patriot Watch Architecture

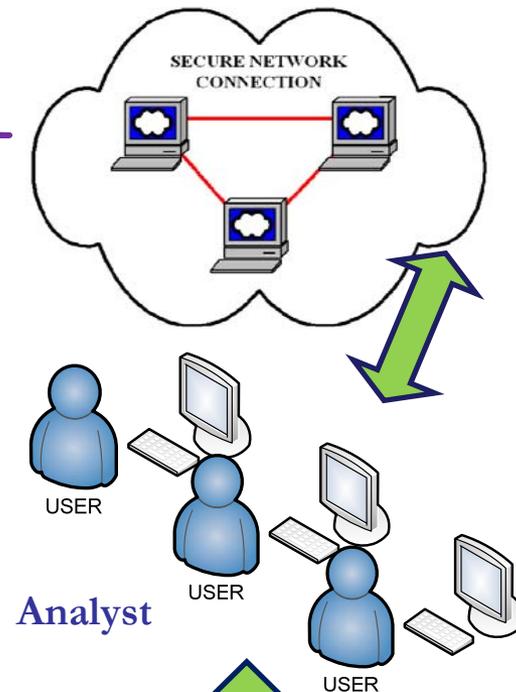
## Monitoring & Collection



## Processing



## Analysis & Evaluation



J-Alert  
CTL-3500



# PNT Monitor overview

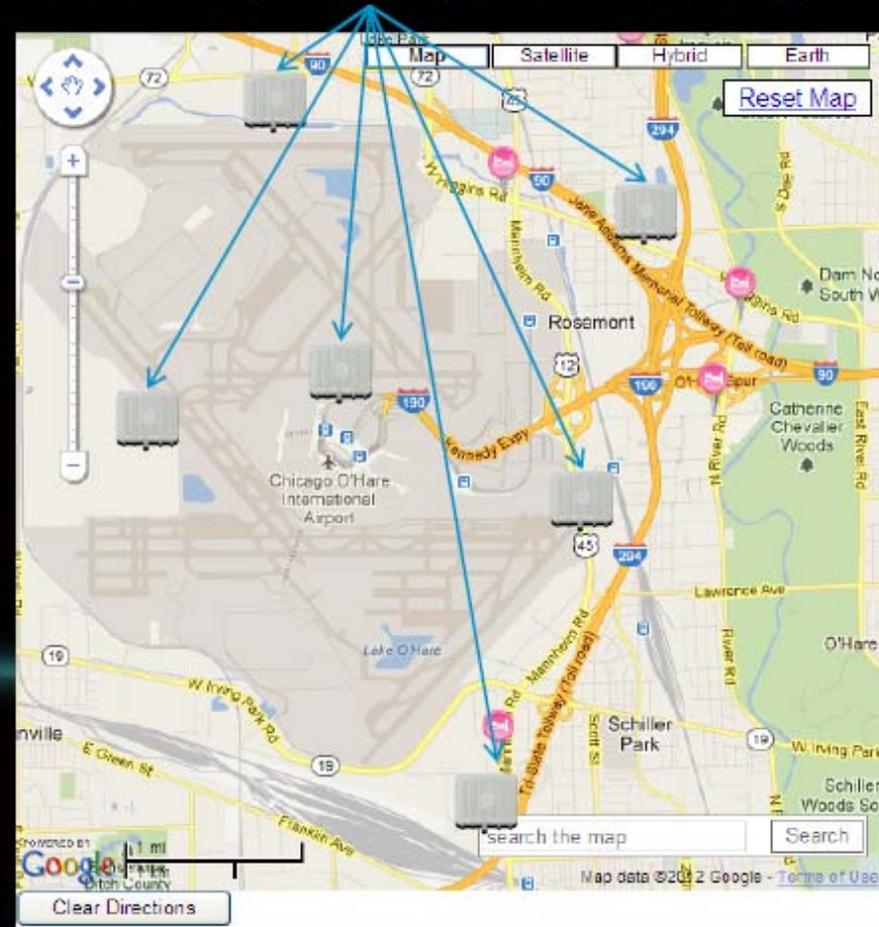
## Agilent 'minnow' system: typical hardware installation

PNT monitor locations selected to detect illegal transmitters along common access routes adjacent to sensitive PNT support equipment.

Information is networked back to central monitoring and alert via UNITRAC.

Information monitored and acted on by FAA agents.

### PNT Monitoring points (Agilent N6841A)

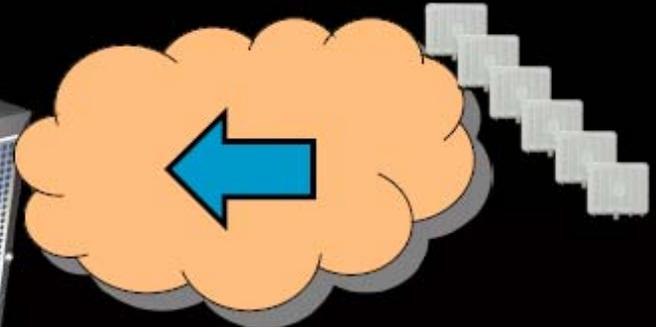
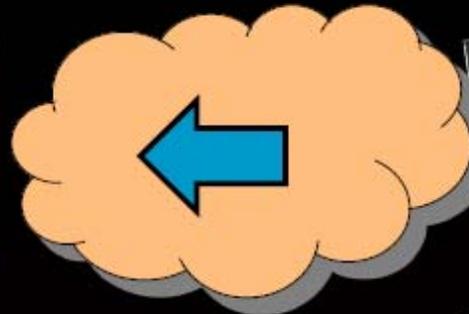
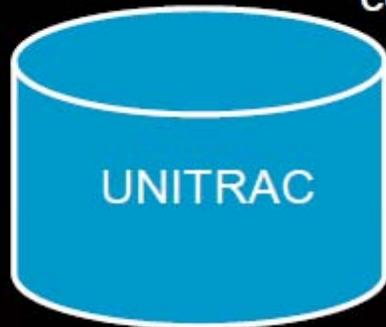


# PNT Monitor overview

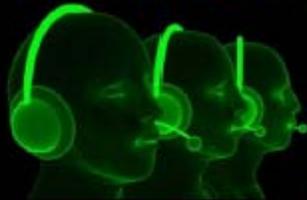
## Agilent 'minnow' system: software architecture

Alarms formatted into  
common UNITRAC messages

PNT Monitor Points



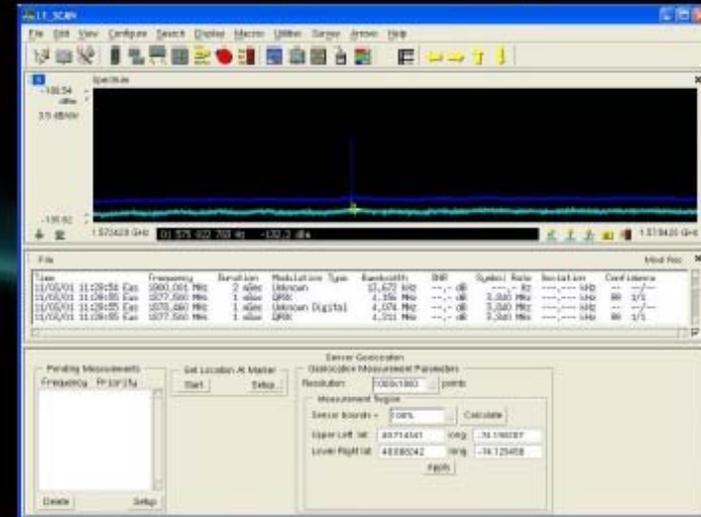
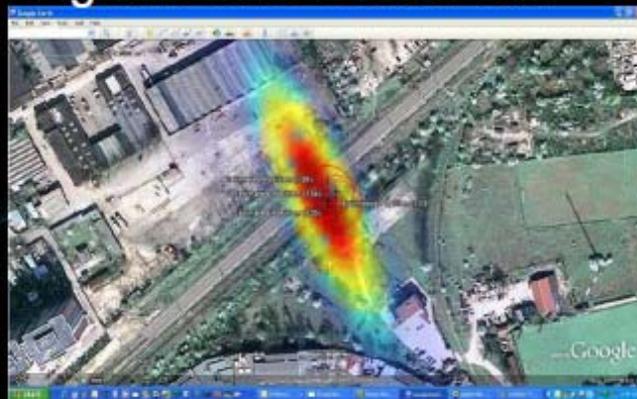
UNITRAC Analysts



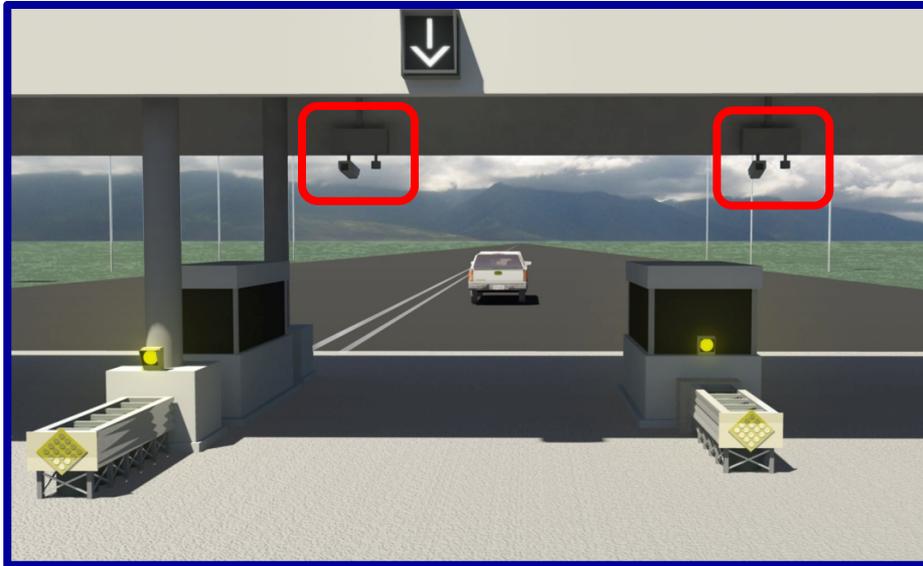
PNT  
Surveyor &  
Location  
Server

Agilent Signal Surveyor SW

Agilent GEO Server SW



# Jammer Geo-Location Port Of Entry Concept



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



# chromos TECHNOLOGY



## J-ALERT

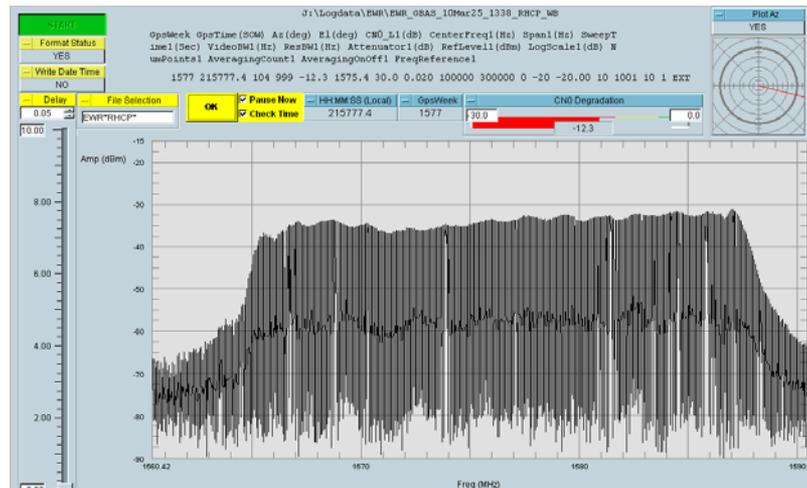
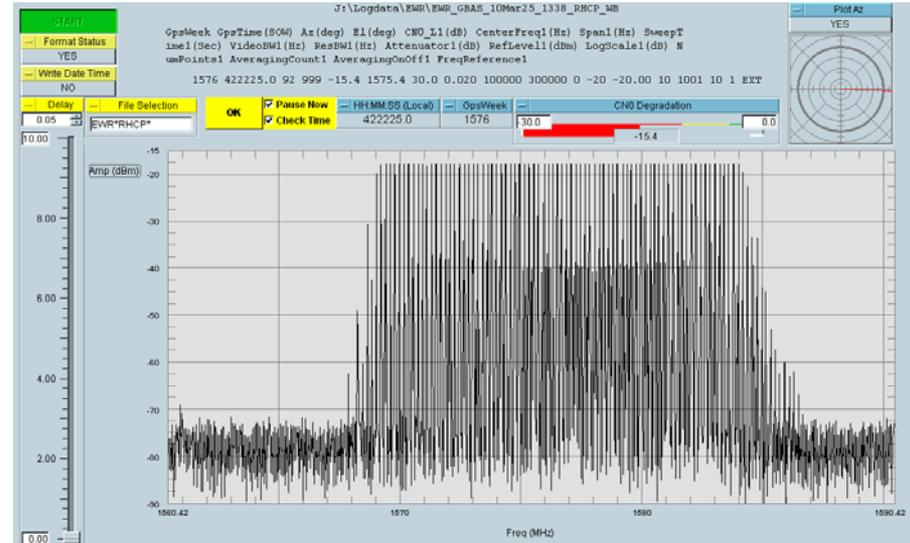
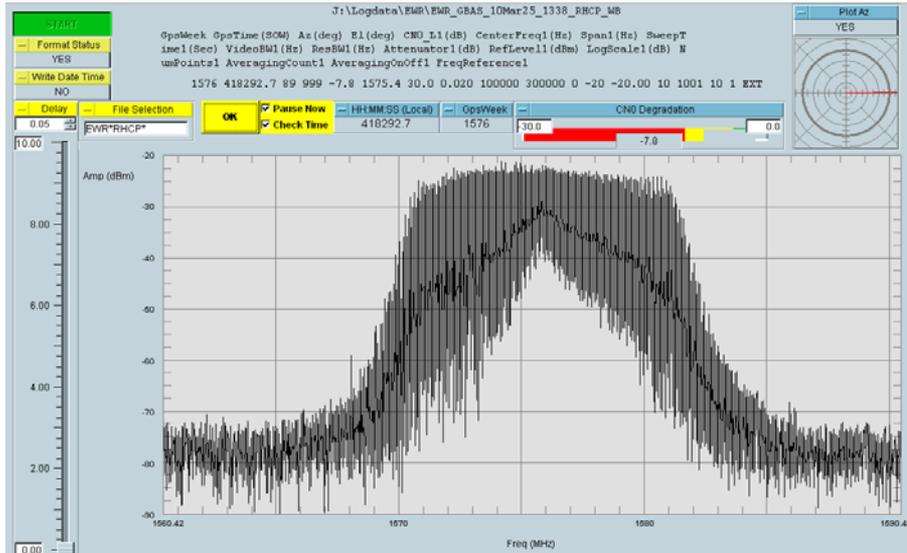
Radio Frequency Jammer Detector

**DYPLEX**  
COMMUNICATIONS LTD

**brimtek**



# GPS Jammer Source Signal Characteristics – Digital Library



# PNT Collaboration Sites



## Homeland Security Information Network

Welcome to HSIN

User Name:   
Password:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored on this information system. The government may disclose or use any communications or data transiting or stored on this information system for any lawful government purpose, including but not limited to law enforcement purposes. You are NOT authorized to process classified information on this system.

DO NOT PROCESS CLASSIFIED INFORMATION ON THIS SYSTEM

U.S. Department of Homeland Security

### PNTIP Application Login Page



Login Email:

Password:

[Change password?](#) [Lost password?](#)

Warning: This is a Federal Aviation Administration (FAA) computer system. [1370.79a](#)

This computer system, including all the related equipment, networks and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. FAA computer systems may be monitored for all lawful purposes, to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify the security of this system.

During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this FAA computer, authorized or unauthorized, constitutes consent to monitoring of this system.

Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.



# Conclusion

- **FAA, FCC, DHS and other Government agencies working closely to address PNT IDM**
- **Collaboration and teamwork is key to successful PNT IDM**
- **Leverage existing mature technologies and collaborate to obtain interference data**
- **Collecting data to support formal analysis; trends on jammers**
- **Research is underway for alternative sources of time**



# QUESTIONS?

[John.Merrill@dhs.gov](mailto:John.Merrill@dhs.gov)

(202) 447-3731 PNT PMO

(202) 731-9628 Mobile

