# PATRIOT WATCH

## INTERFERENCE DETECTION MITIGATION (IDM)

## VIGILANCE

## SAFEGUARDING AMERICA

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

**August 14, 2012**

# Interference Detection & Mitigation (IDM) per NSPD 39

- Identify
- Analyze
- Locate
- Attribute
- Mitigate

# Existing and Emerging Threats



**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

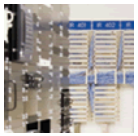

Defense Industrial Base


Emergency Services


Energy *

Government Facilities


Healthcare and Public Health


Information Technology *

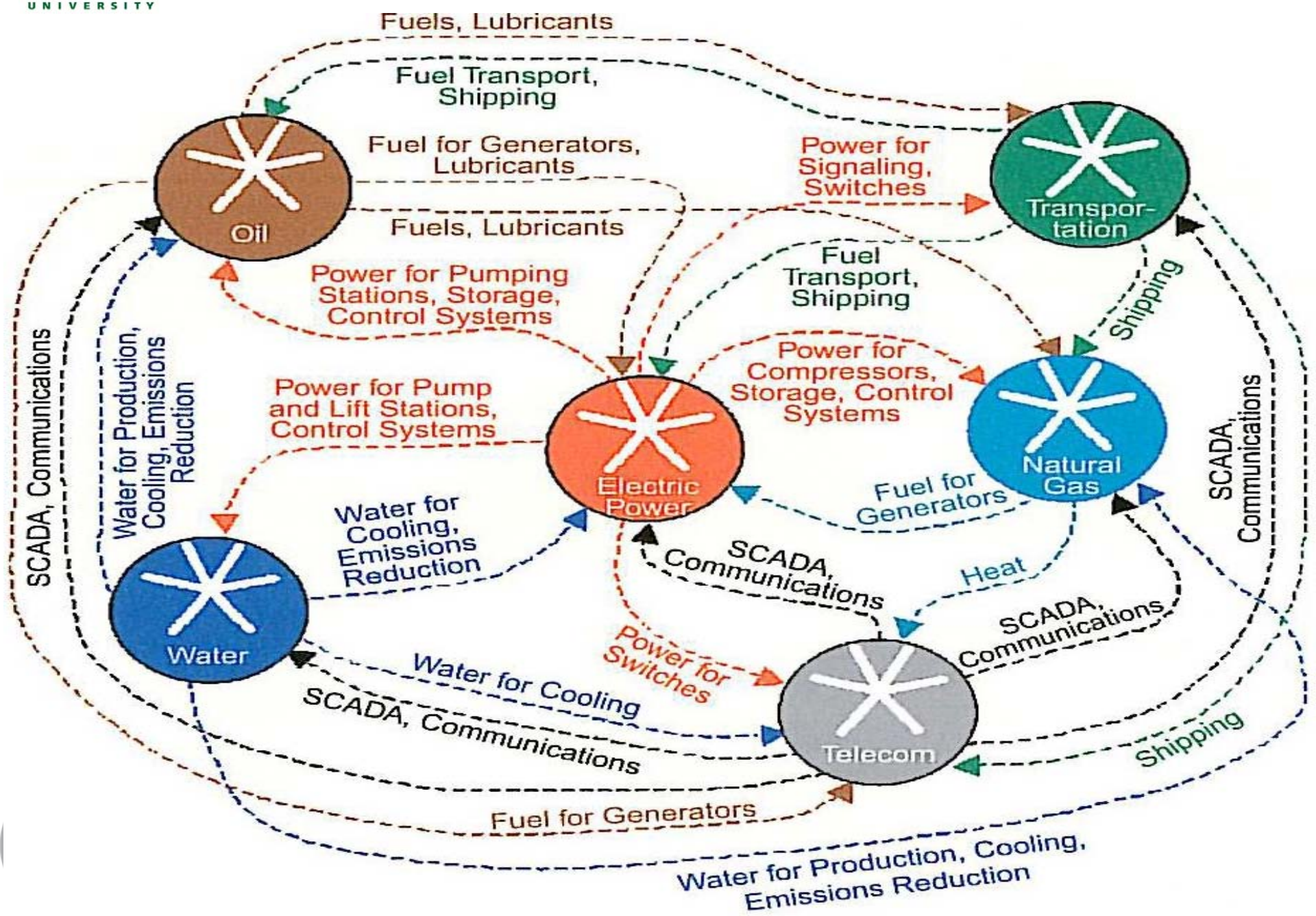

National Monuments and Icons


Nuclear Reactors, Materials and Waste


Postal and Shipping


Transportation Systems

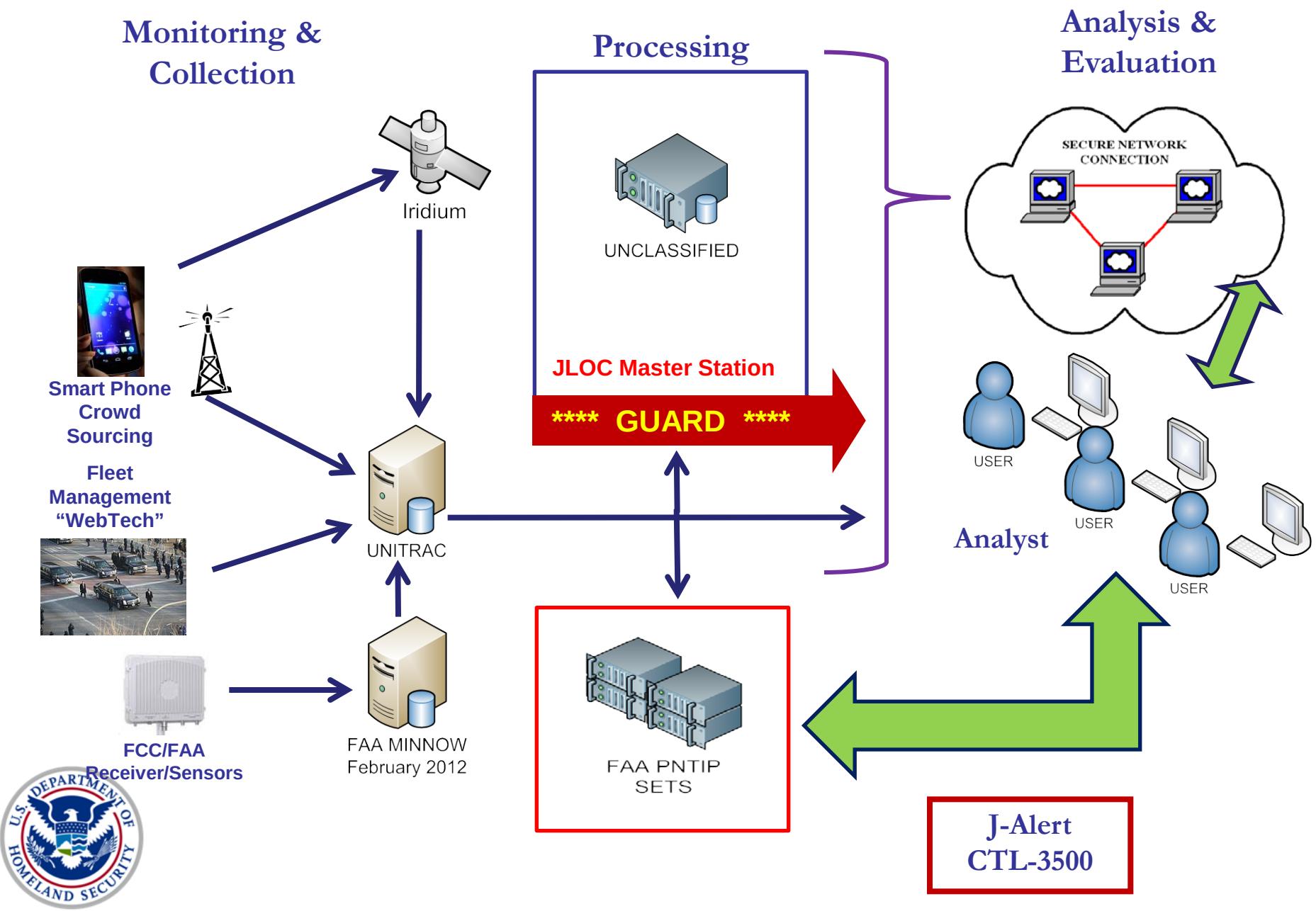

Water


Fuels, Lubricants
Fuel Transport, Shipping
Fuel for Generators, Lubricants
Fuels, Lubricants
Power for Signaling, Switches
Oil
Transpor-tation
Power for Pumping Stations, Storage, Control Systems
Fuel Transport, Shipping
Shipping
Power for Compressors, Storage, Control Systems
Power for Pump and Lift Stations, Control Systems
Water for Production, Cooling, Emissions Reduction
SCADA, Communications
Electric Power
Natural Gas
Fuel for Generators
SCADA, Communications
Water for Cooling, Emissions Reduction
SCADA, Communications
Heat
SCADA, Communications
Water
Power for Switches
Water for Cooling
SCADA, Communications
Telecom
Shipping
Fuel for Generators
Water for Production, Cooling, Emissions Reduction

# 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



# 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.

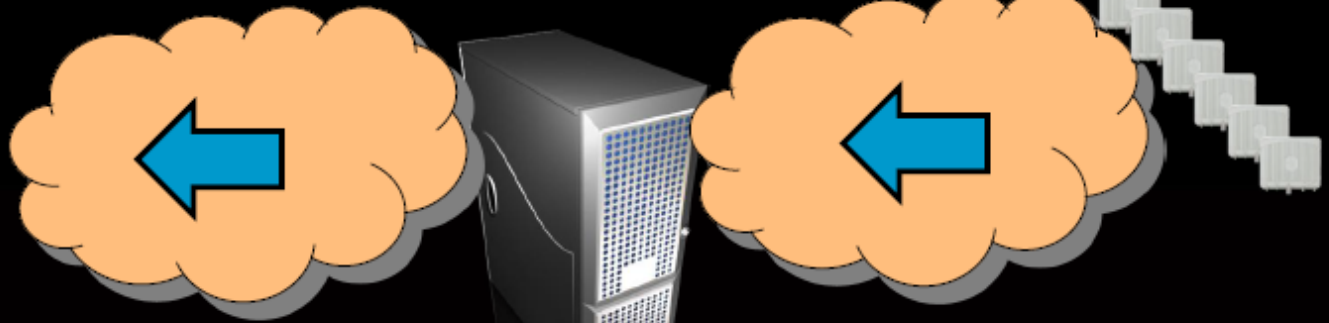
PNT Monitoring points (Agilent N6841A)

# PNT Monitor overview

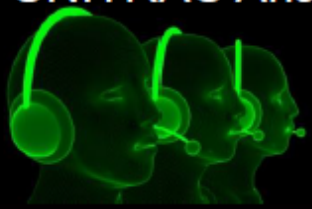
## Agilent 'minnow' system: software architecture

Alarms formatted into
common UNITRAC messages

PNT Monitor Points

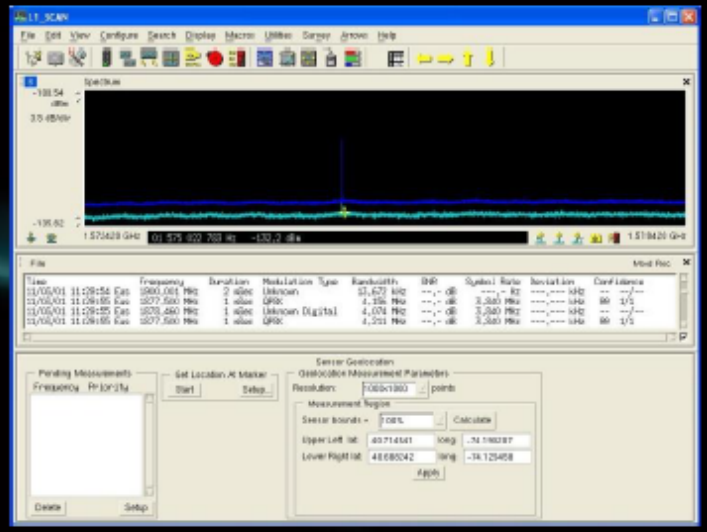



UNITRAC Analysts

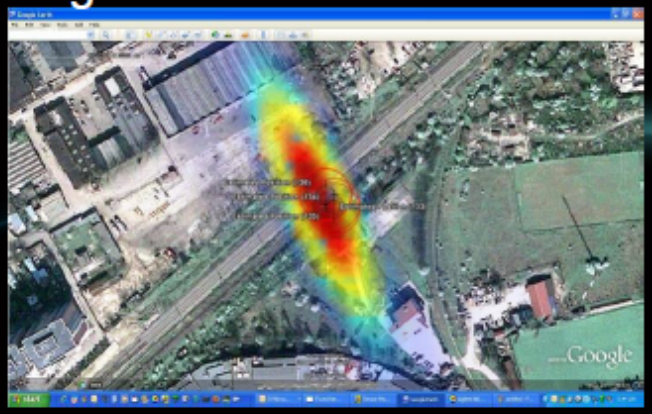


PNT
Surveyor &
Location
Server

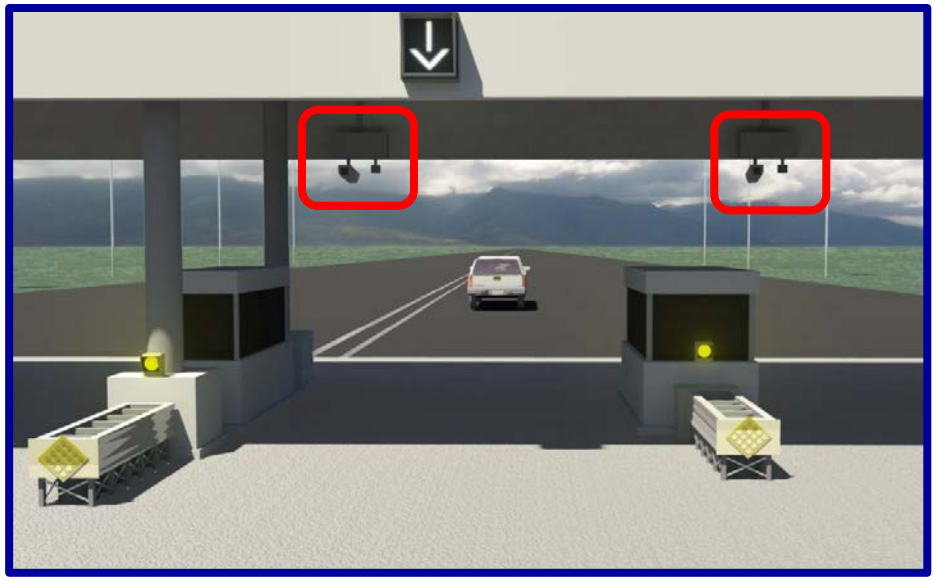
Agilent Signal Surveyor SW

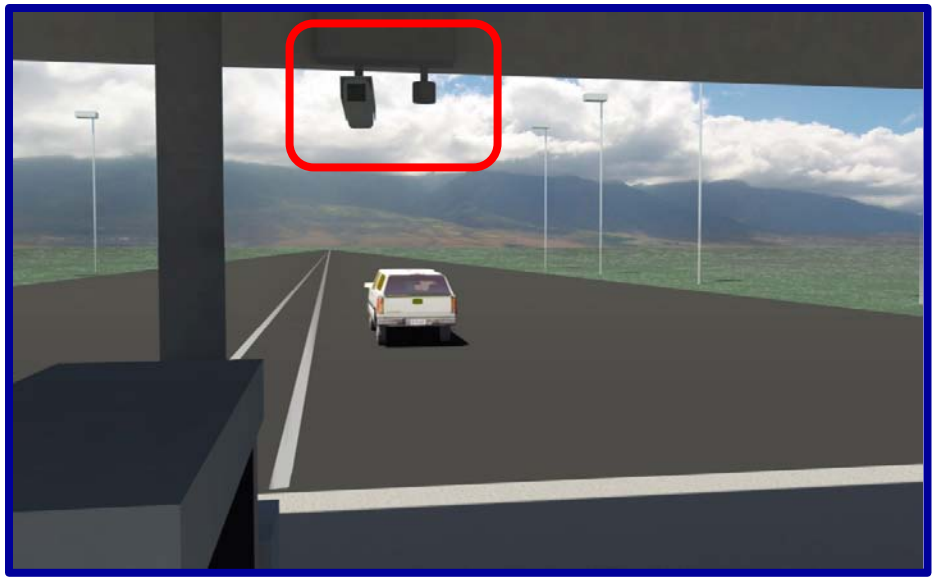


Agilent GEO Server SW



# Jammer Geo-Location
# Port Of Entry Concept



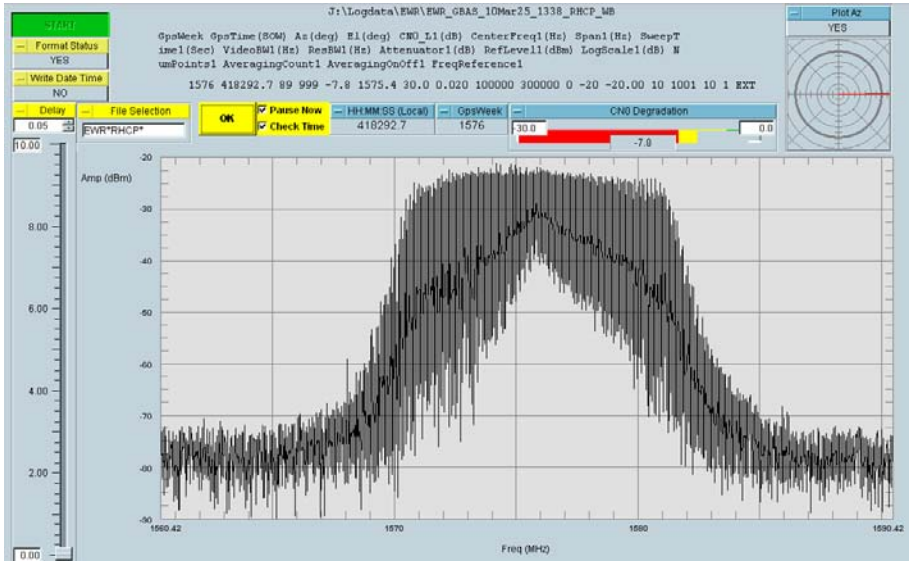


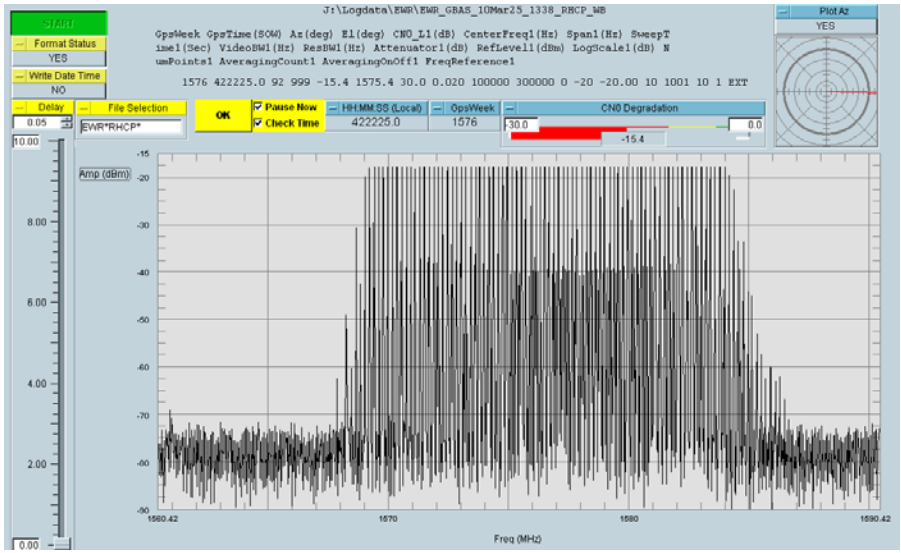
- Integrated with Camera System
- Alert Enforcement Personnel to Jammer Presence
- Detect & Track Jammers Approaching Entry Point
- Multi-Lane Distinction
- UNITRAC Database Connection

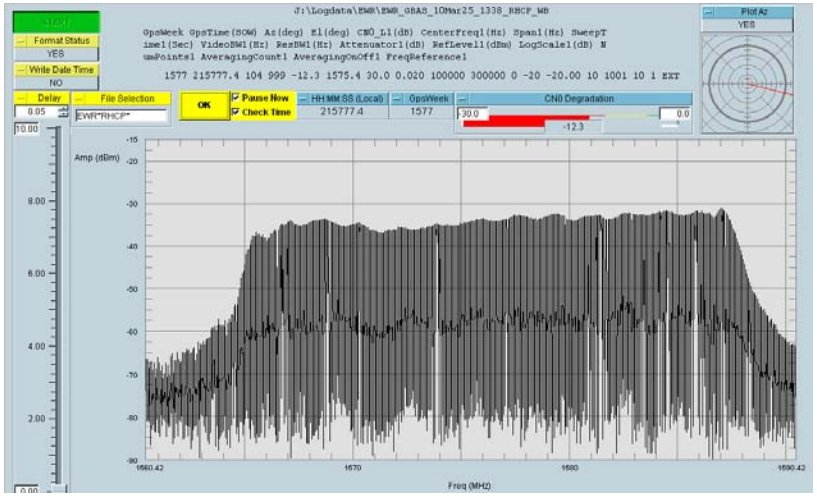
chronos

TECHNOLOGY


# GPS Jammer Source Signal Characteristics – Digital Library



# PNT Collaboration Sites


# 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

(202) 447-3731 PNT PMO

(202) 731-9628 Mobile