

Patriot Watch

VIGILANCE

SAFEGUARDING AMERICA

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

WSTS March 2012



**Homeland
Security**

Agenda

- **Governance/FCC Regulations**
- **Existing and Emerging Threats**
- **Critical Infrastructure Dependencies**
- **Patriot Watch Architecture**
- **Sensor/Data Integration, UniTrac**
- **Case Studies of Incidents**
- **Technology Research**
- **PNT Collaboration Sites**
- **Conclusions**



Homeland
Security

Interference Detection & Mitigation (IDM) per NSPD-39

- Identify
 - Analyze
 - Locate
 - Attribute
 - Mitigate



Homeland
Security

NSPD: National Security Presidential Directive



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



Homeland
Security

Existing and Emerging Threats



A screenshot of an e-commerce website. The top navigation bar includes categories like 'Apple Accessories', 'Computers & Peripherals', 'Cell Electronics', 'Car Electronics', 'Security & Surveillance', 'Entertainment', 'Health & Lifestyle', 'Cameras & Photo', and 'Batteries & Chargers'. A 'Categories' sidebar on the left lists 'Security & Surveillance', 'Jammers', 'Door Phones', 'Surveillance Cameras', 'DVR Cards & Systems', 'Cell Phone Booster', 'Baby Monitors', and 'Baby Safety & Health'. The main content area features a 'Cell Phone Signal Jammer | GPS Blocker' section with an 'AMAZING DEAL!' banner for a 'Portable Cell Phone GPS Jammer' priced at US\$36.99 (down from US\$73.98) with a 50% off badge. To the right is a 'WEEKLY DEAL' for a '1600MHz GPS Signal Jammer' for US\$25.99 (down from US\$35.99) with a 'SAVE \$10' badge. Below these are four smaller product thumbnails.

About 500,000 hits on “GPS Jammer”



Homeland Security

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](#)



Homeland Security

Extent of GPS Dependencies

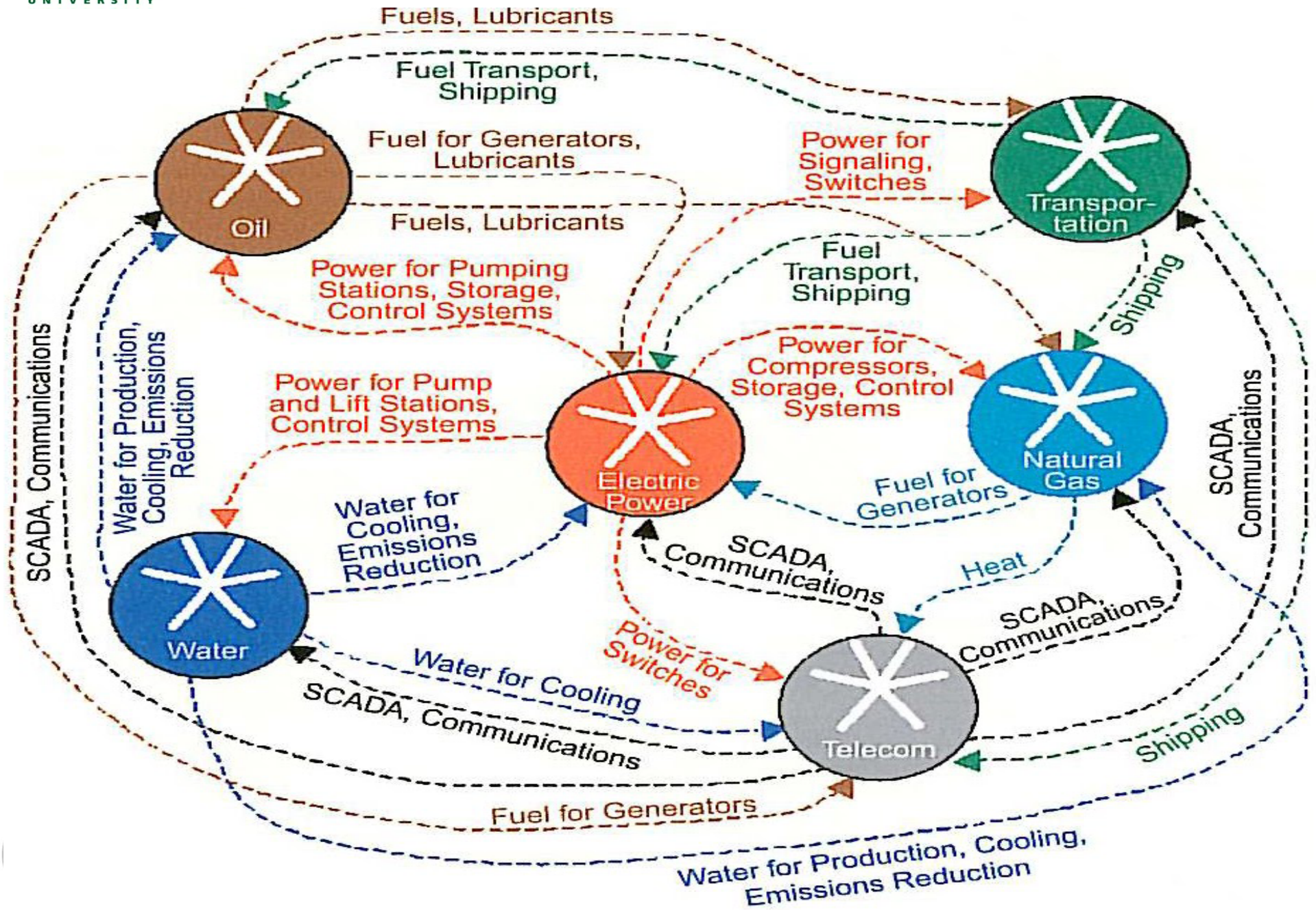


GPS Supporting Power Grid Systems

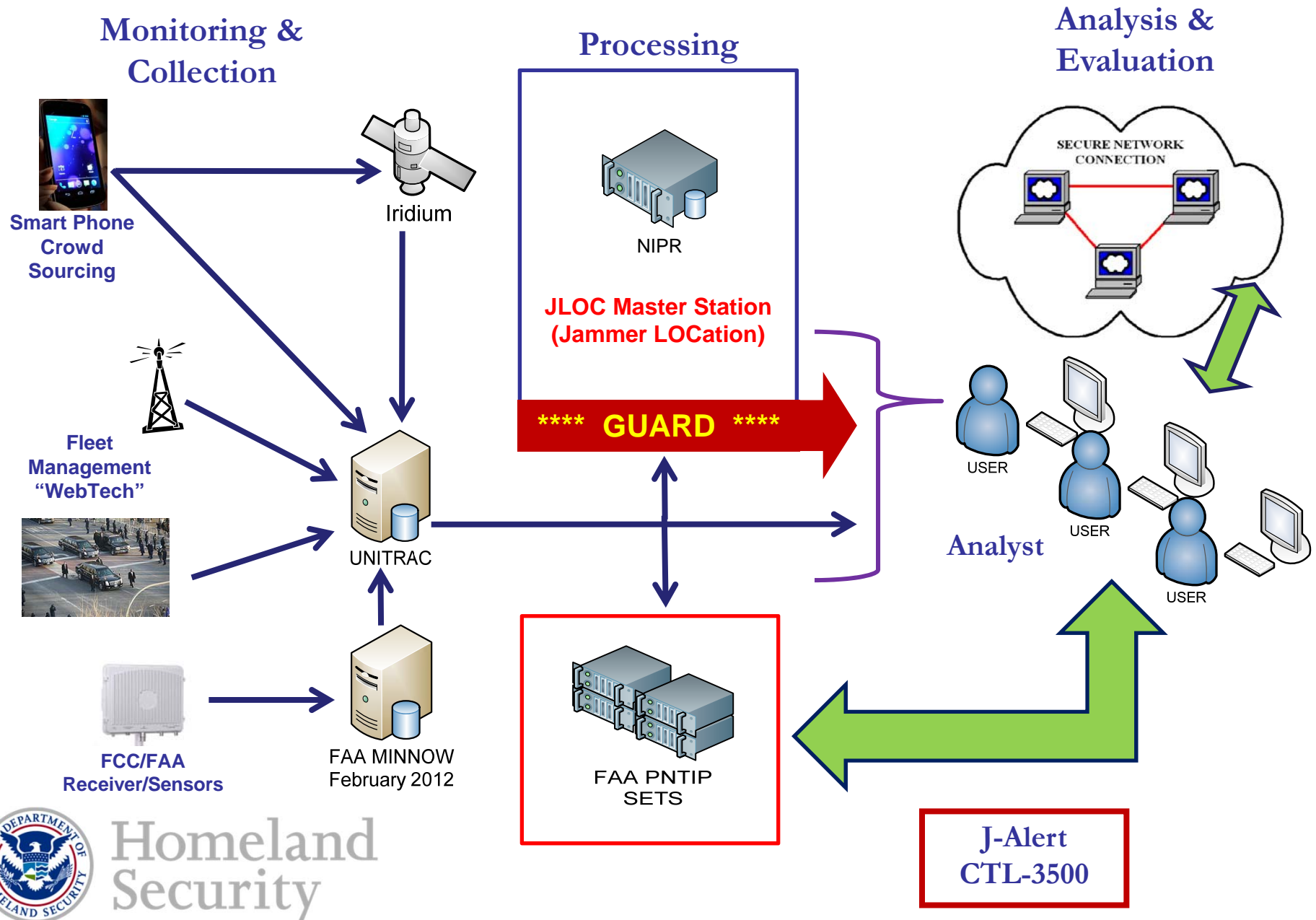
GPS Supporting Banking Operations

GPS Supporting Transportation Systems

GPS Supporting Communications Systems



Patriot Watch Architecture



Patriot Watch Standard Data Set

CIVIL GPS MONITOR SYSTEM Version 1.0

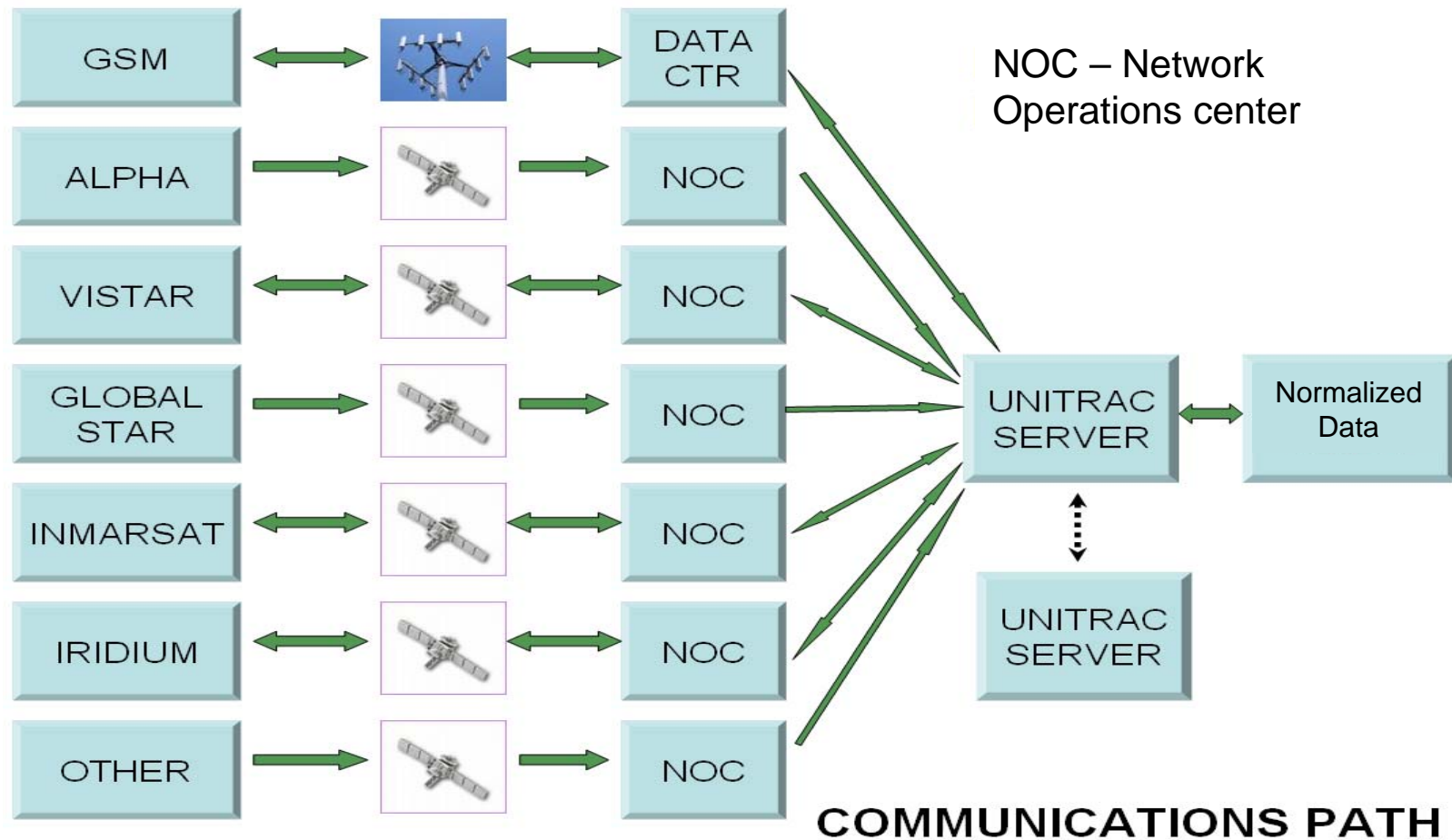
SERVER REPORT MESSAGE - Event Data XML Message (Non- Proprietary)

Item	Req/Opt	Data Field	Schema	Example(s)
1	Required	Report Type	Constant	GPS disruption
2	Required	version	Mask: #.#a	1.0a
3	Required	Source	enum: TelcoGPS, CORS, WAAS	WAAS
4	Required	Report time	Date/Time: Zulu	01152010.0915Z
5	Required	Event ID	Mask: ####.#####.###	Series.event.sequence 0000.000001.001
6	Required	Event Type	enum: Real, Test, Exercise	Exercises
7	Required	Classification	enum: Unclassified, Secret, Top Secret	Unclassified
8	Required	Signal Affected	enum: L1, L2C, L5, E5a, E5b, E6, Glonass	L1
9	Required	Signal Status	enum: Signal Loss, Time fault, Location Fault, Maint, Mixed	Signal Loss
10	Optional	Region	String	Region/Area affected: City, State, CONUS
11	Required	Sites Reporting	Integer: 0 - 300,000	15
12	Required	Spatial Profile	enum: Ground, Air, Space, Unknown	ground
13	Required	Spatial Status	enum: Static, Moving, Growing, Shrinking, Unknown	Static
14	Required	Temporal Profile	enum: Simultaneous, Random, Intermittent, Unknown	Simultaneous
15	Required	Temporal Status	enum: In Progress, Ended	In Progress
16	Required	pattern	enum: Omni, Directional, Unknown	Omni
17	Required	Estimated ERP (dBm)	Single: 0 - 10,000	100
18	Required	Icon	Bitmap(Blob)	x by x bitmap
19	Required	Centroid Latitude	Single: -90 to +90 Degrees	+/- xx.xxxx
20	Required	Centroid Longitude	Single: -180 to +180 Degrees	+/- xxx.xxxx
21	Optional	Impact Area Polygon	List: Lat, Long	+/-xx.xxxx, +/- xxx.xxxx
22	Optional	Source Area Polygon	List: Lat, Long	+/-xx.xxxx, +/- xxx.xxxx
23	Optional	Event Start Time	Date/Time: Zulu	01152010.0911Z
24	Optional	Event Stop Time	Date/Time: Zulu	01152010.0911Z
25	Optional	Note / Details	Text Blob	Extra Details



Homeland
Security

UNITRAC ARCHITECTURE



Homeland
Security

Moss Landing, CA



FIGURE 2 search bearing for Source-1



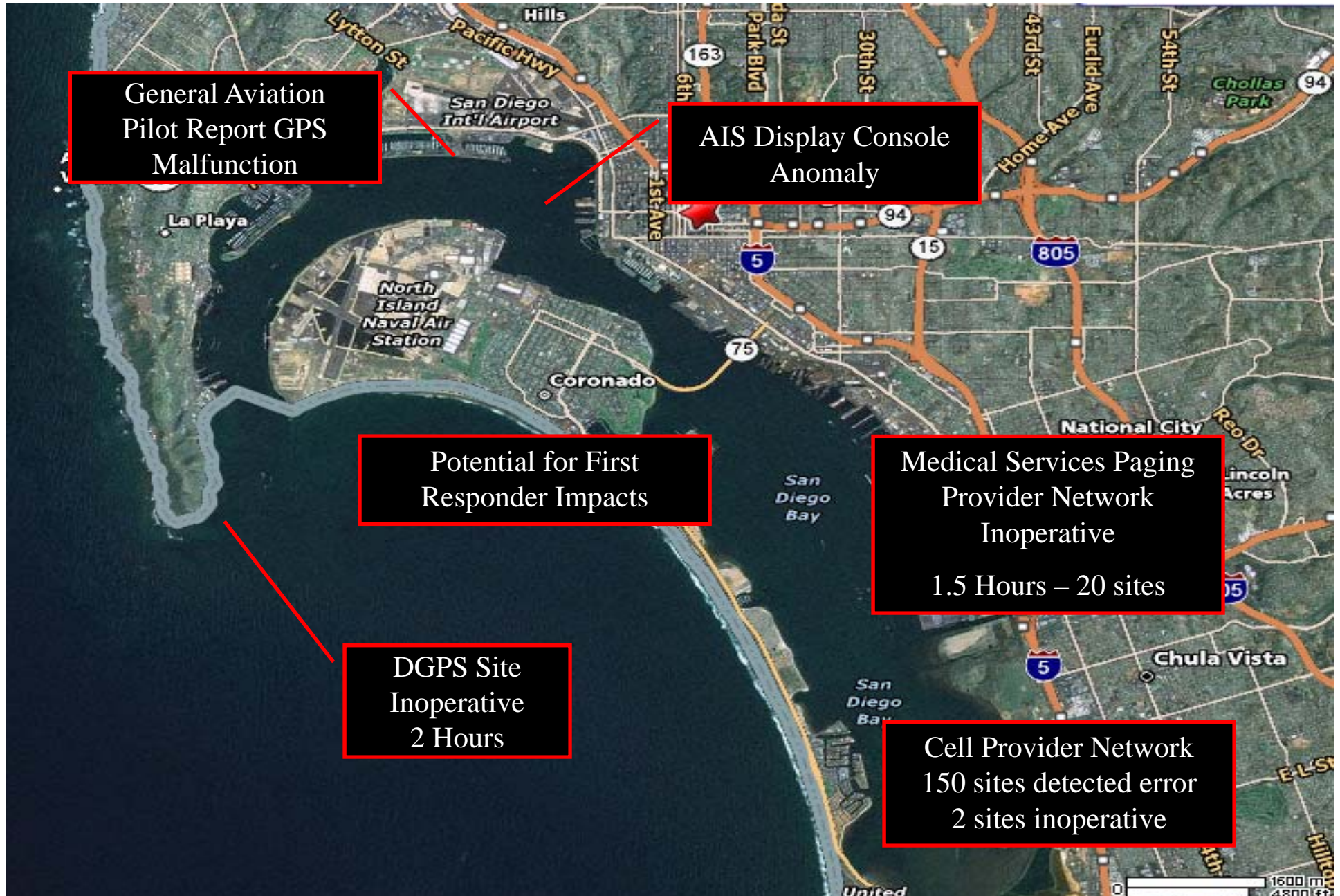
Courtesy of GPS World, January 1, 2003. "The Hunt for RFI" W.R. Vincent, R.W. Adler, P. McGill, J.R. Clynch, G. Badger, A.A. Parker.

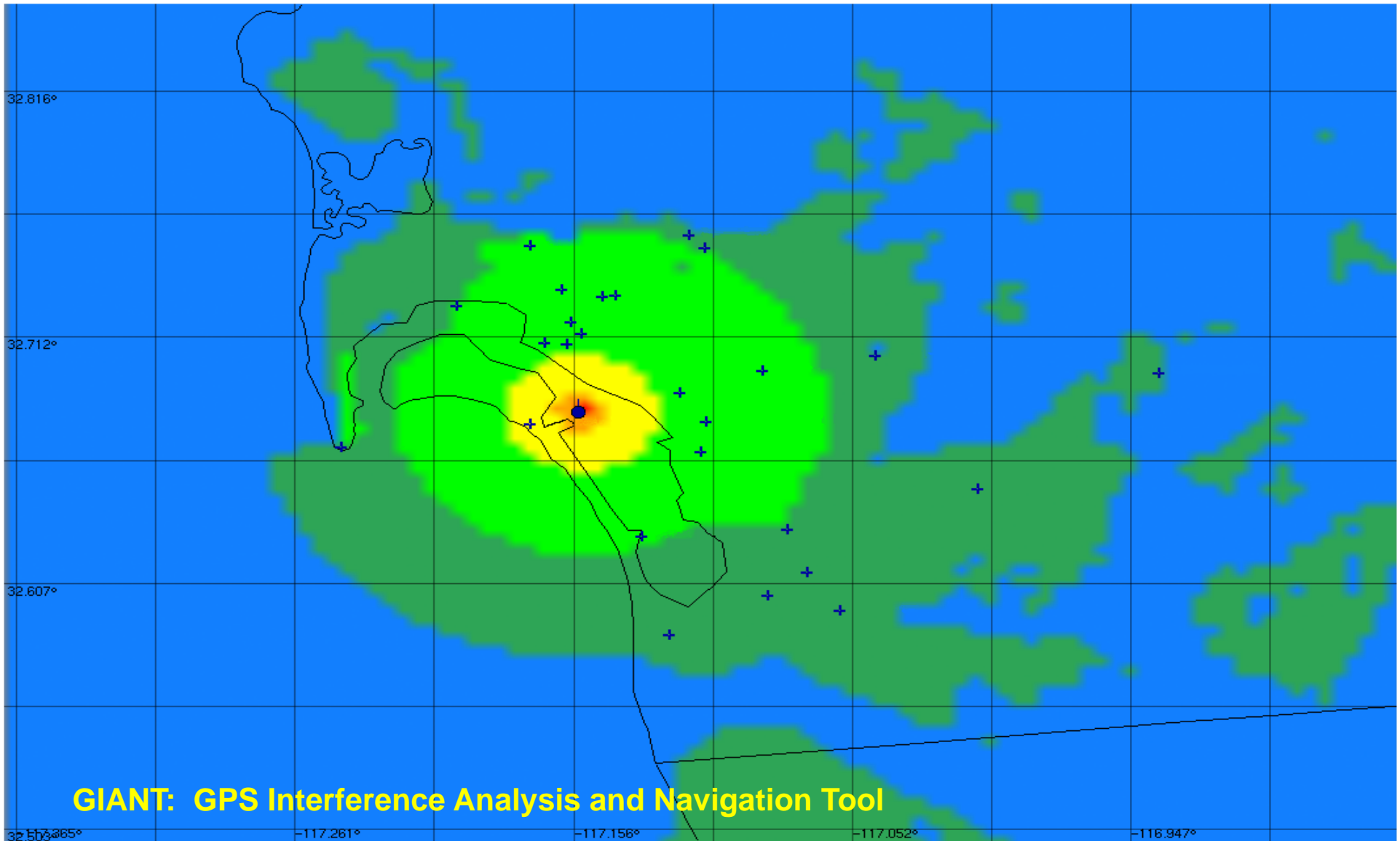


U.S. DEPARTMENT OF
HOMELAND SECURITY

Homeland Security

San Diego January 2007





GIANT: GPS Interference Analysis and Navigation Tool

Contour Legend

Metric: CA-L1 Altitude: 100 ft AGL
 Production Date: 01/24/2007 22:33:56 Latitude Increment: N 0.00400000°
 Almanac File: SEM week 387 Longitude Increment: E 0.00500000°
 Scenario: 22 Jan 2007 Outage Number of Channels: 14
 Route: New J2S Contour Mask Angle: 5°
 Start Time: 23 Jan 2007 22:23:15 Signal Modulation: BPSK
 End Time: 23 Jan 2007 22:23:15

	> 90.0 dB		40.0 - 50.0
	80.0 - 90.0		30.0 - 40.0
	70.0 - 80.0		20.0 - 30.0
	60.0 - 70.0		10.0 - 20.0
	50.0 - 60.0		0.0 - 10.0

No Outages

The FAA First Detection – Identify

→ November 23, 2009 during initial SLS-4000 stability testing the Station Faulted and Reference Receiver Satellite Tracking was Interrupted.

SLS-4000 Components

GPS Antenna (RRA)

- Multipath Limiting design
- Sharp cutoff/rejection at horizon

GPS Receiver (RSMU)

- 48-channel, L1 C/A GPS
- Signal Deformation Monitoring (SDM) capable



VHF Radios (VDB)

- D8PSK modulation, TDMA
- Nav band, 108-118 MHz

VHF Antenna

- Horizontal (HPOL) or Elliptical (EPOL) polarized signal



Processor HW (DCP)

- Pentium M, 1.8 GHz CPU
- Hosts integrity monitoring software

Processor SW (DCP)

- Real time monitoring for GPS failure modes, local error sources
- Differential correction determination
- User interface via Maintenance Data Terminal

DCP: Differential Correction Processor
RPDP: Robust Power Distribution Panel
VHF: Very High Frequency
VDB: VHF Data Broadcast
HW: Hardware
RRA: Reference Receiver Antenna
RSMU: Remote Satellite Measurement Unit

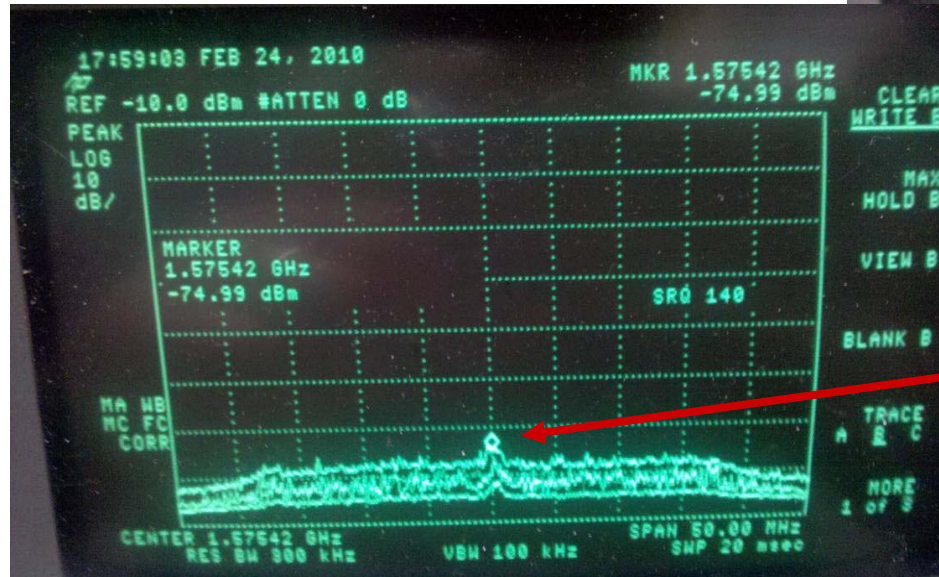
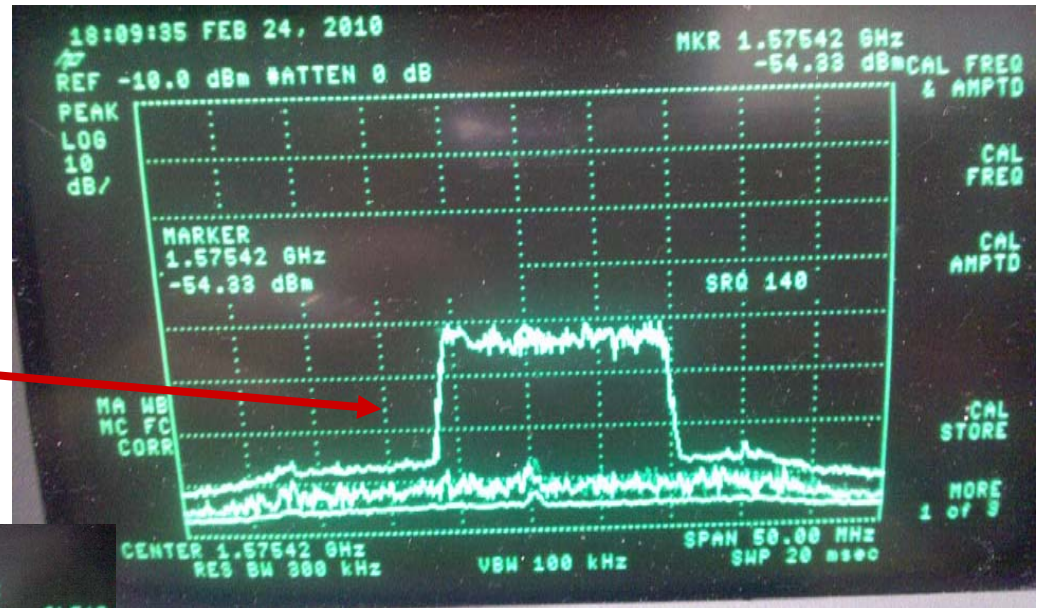


Homeland
Security

FAA Spectrum Measurements – Analyze

→ Wideband Intermittent Source detected in December 2011 occupying approx – 20 MHz

→ 5 MHz below and 15 MHz above L1.



→ Normal L1 Pass Band Spectrum when Interference Source is Not Present.



Homeland Security

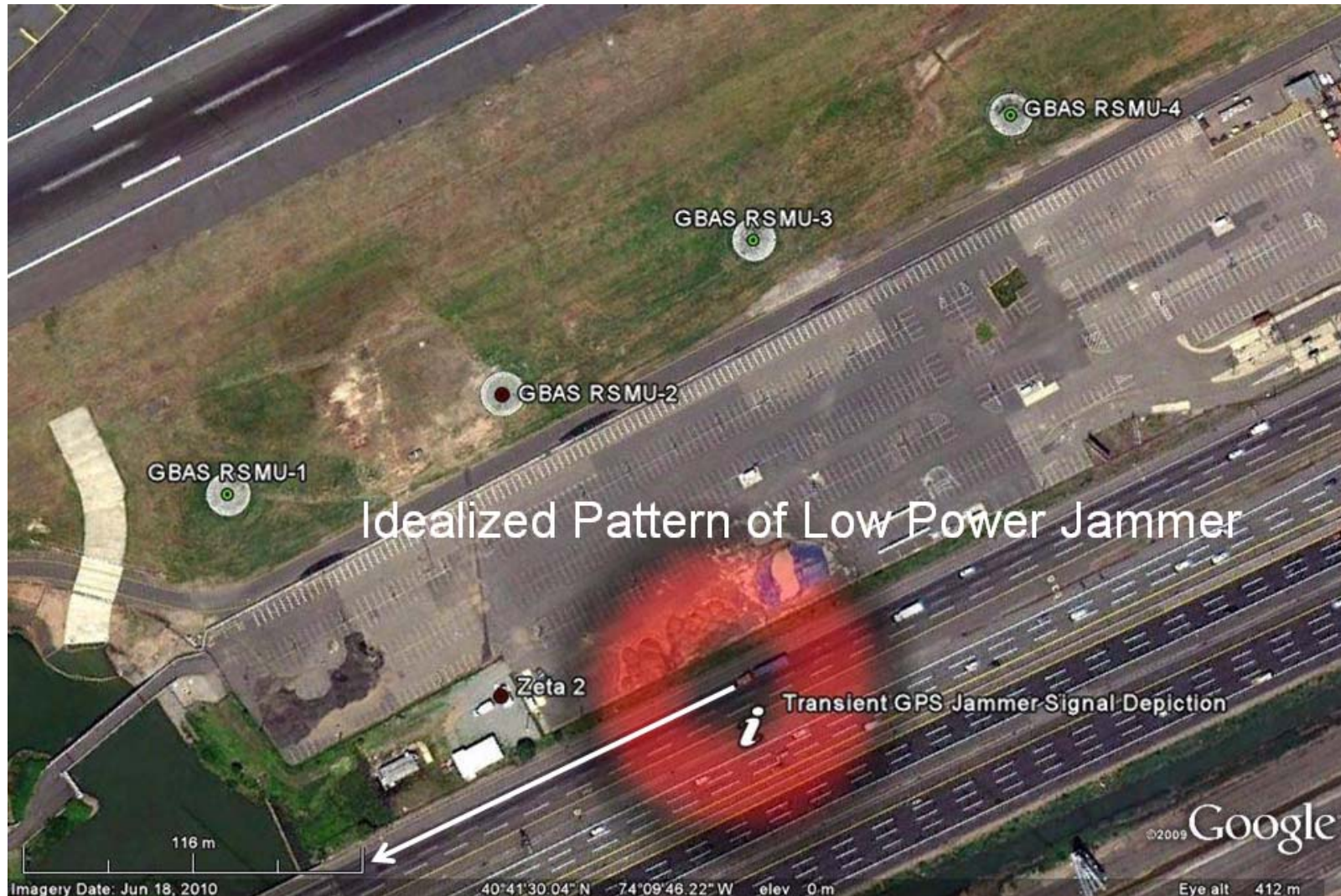
FAA/FCC Investigation

- Government and Contractor Teams convened in Newark on February 24 – 26, 2010 in an attempt to locate the direction toward the source of the observed interference events.
- The Teams on site for the first time had a “Learning Curve” experience and effective data could not be obtained.
 - Three (3) Radio Frequency Interference (RFI) events were observed and measured, but not by all on-site teams.
- The same Teams participated again during March 22 – 25, 2010 in an attempt to draw accurate and more conclusive simultaneous lines of bearing.
 - Measurements and data analysis reveal interference source was MOBILE at slow and fast rates.



Homeland
Security

RFI Source Emission Modeled – Analyze



Homeland
Security

New Jersey Turnpike Overpass Point – Analyze



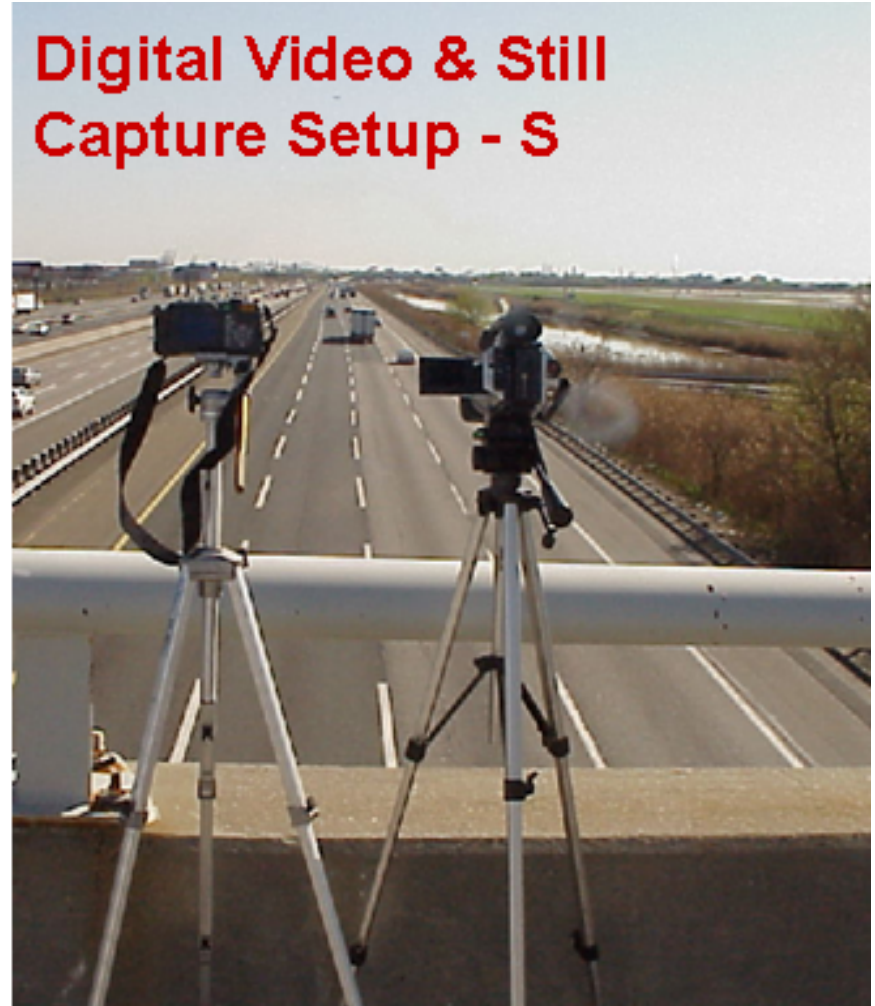
Homeland Security

Equipment Capture Setup – Analyze

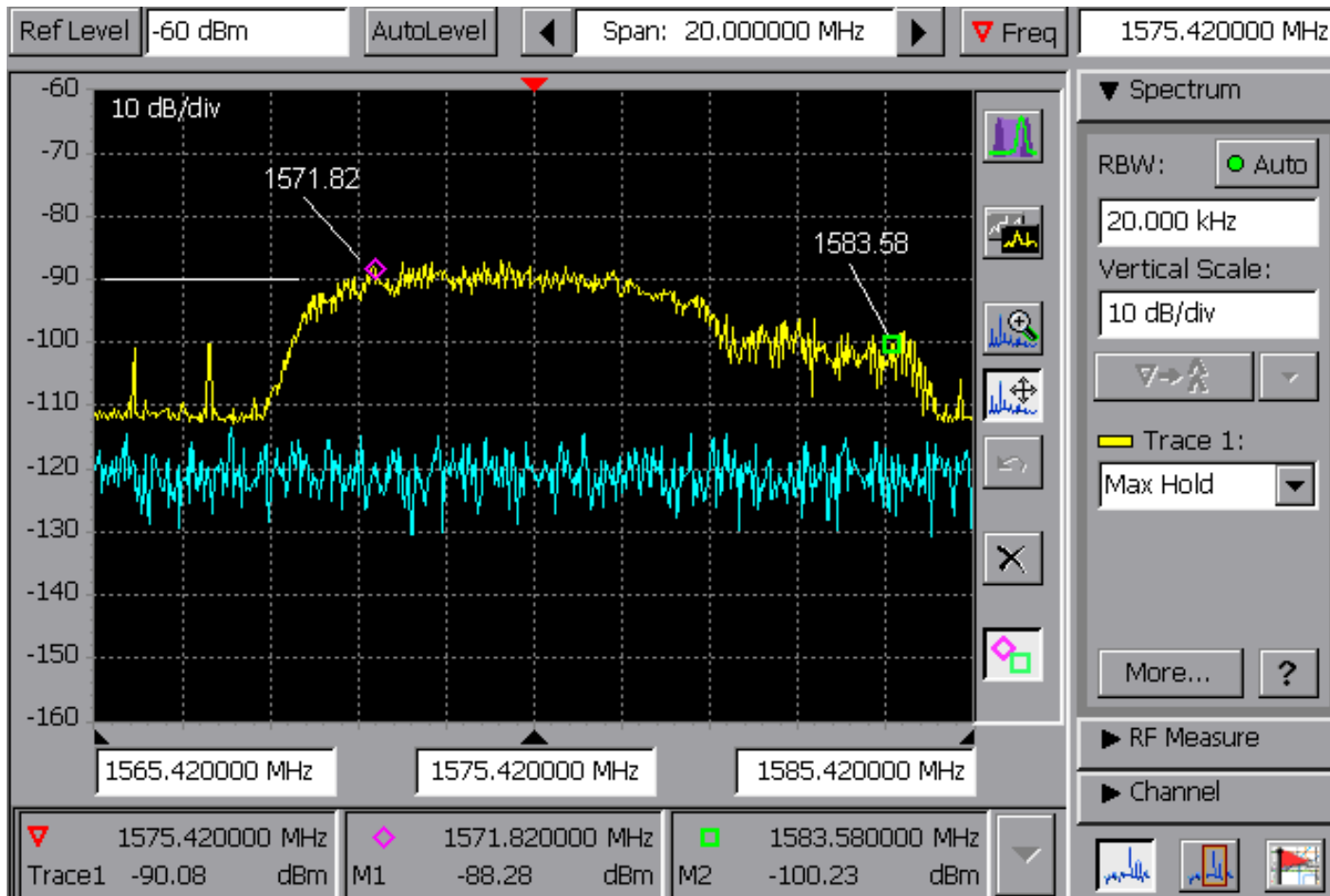
Directional SA Measurement Setup - S



Digital Video & Still Capture Setup - S



Homeland
Security



Date: 04/15/2010 03:29:16 PM

GPS Position: 40° 41' 17.774" N - 74° 9' 49.636" W

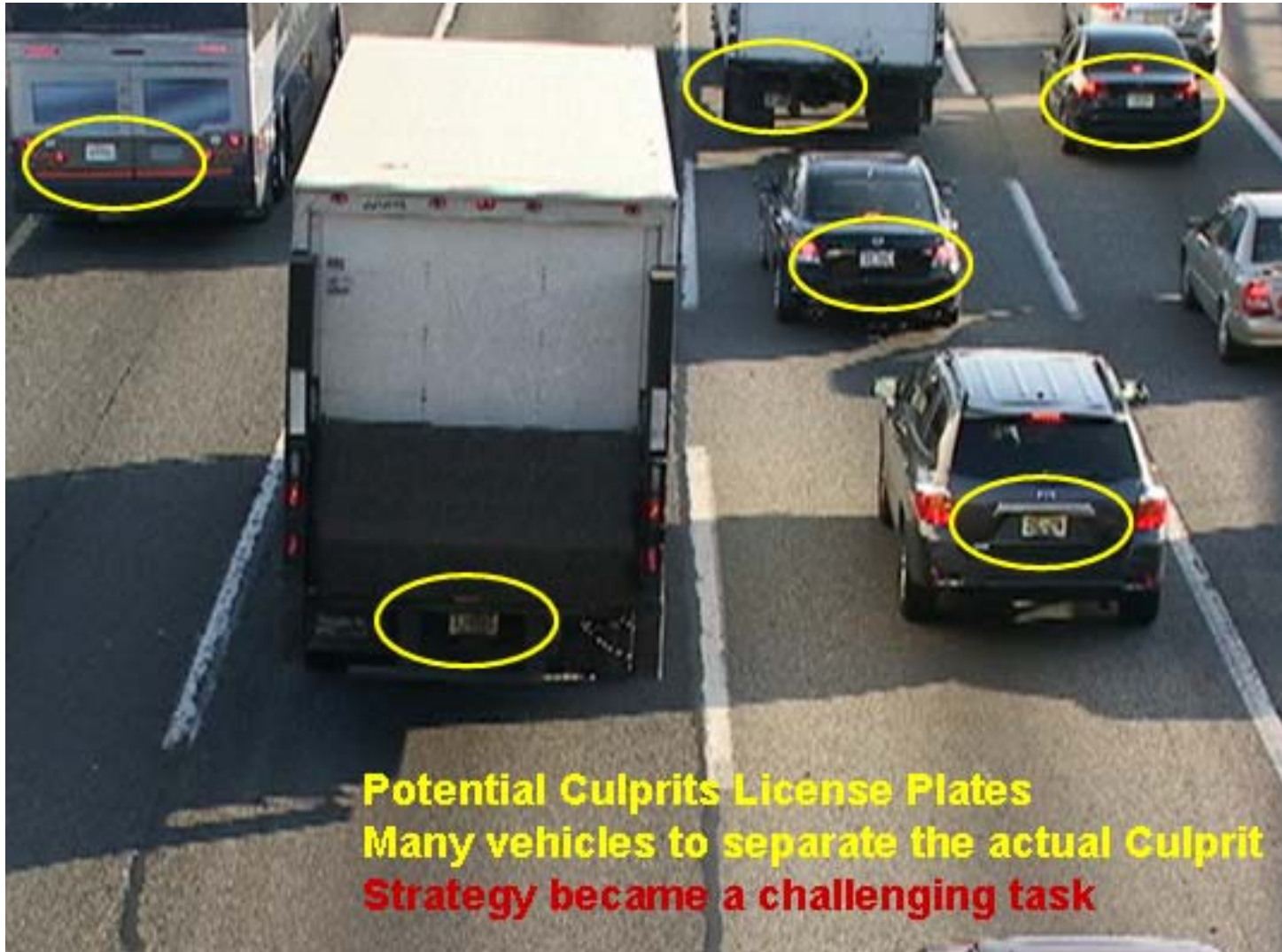
User Name: James S. Aviles

Note: EWR GBAS Interference measured at MP103 Overpass same suspect truck detected in the AM.



Homeland
Security

... so which one is the culprit?



Homeland
Security

GPS RFI Source Pursuit – Locate



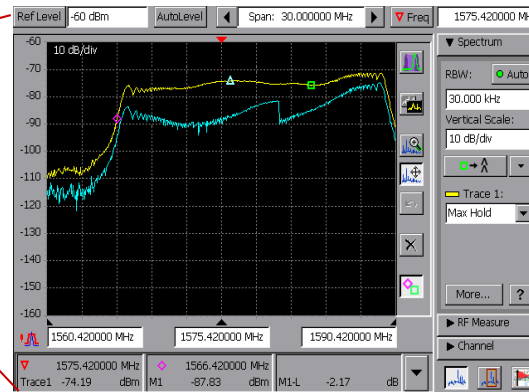
FCC MDDF Ready



FAA RFHawk Ready



FAA "Tip OFF" Ready

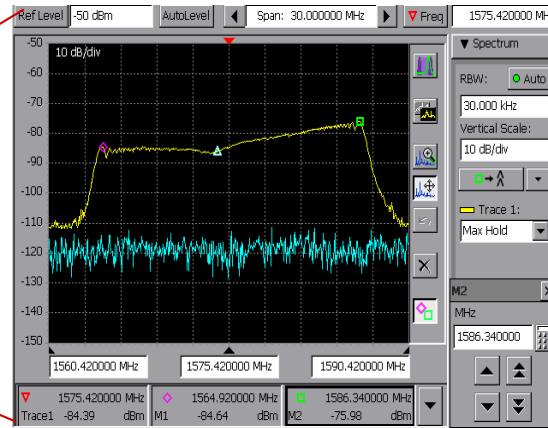


RFI source "Locked-on" and pursued until vehicle stop at traffic light further south pass Exit 13A. See Video.



Homeland Security

GPS RFI Source Unveiled – Locate



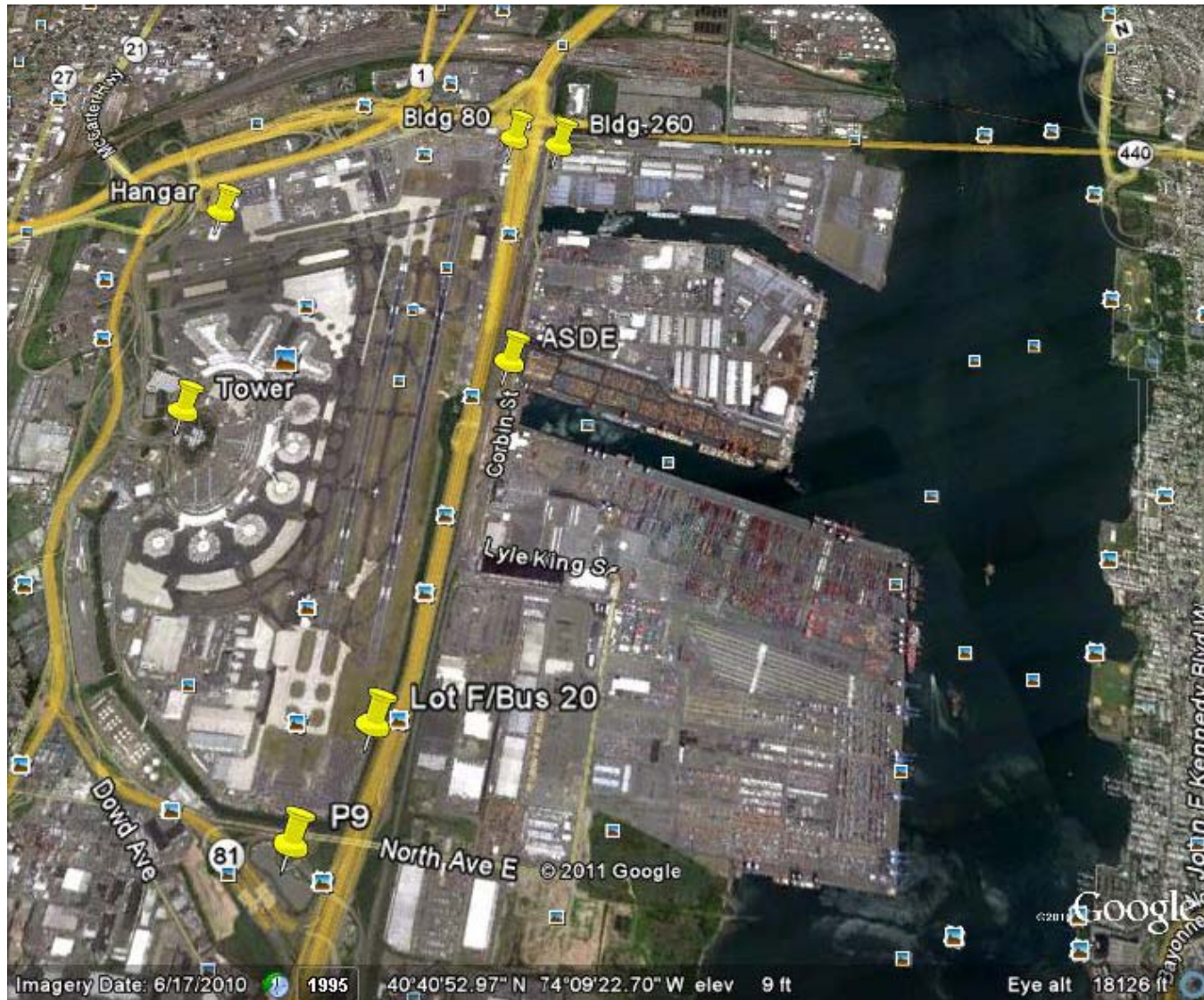
On Site ON-OFF tests confirm surrendered GPS RFI source on April 29, 2010

November 2009 – April 2011 to locate 1 GPS jammer!



U.S. DEPARTMENT OF
**Homeland
Security**

FCC/FAA Minnow Deployment – Locate



Homeland
Security

chronos TECHNOLOGY



J-ALERT

Radio Frequency Jammer Detector

DYPLEX
COMMUNICATIONS LTD

brimtek



U.S. DEPARTMENT OF
HOMELAND SECURITY

Homeland Security

International Partners Capability

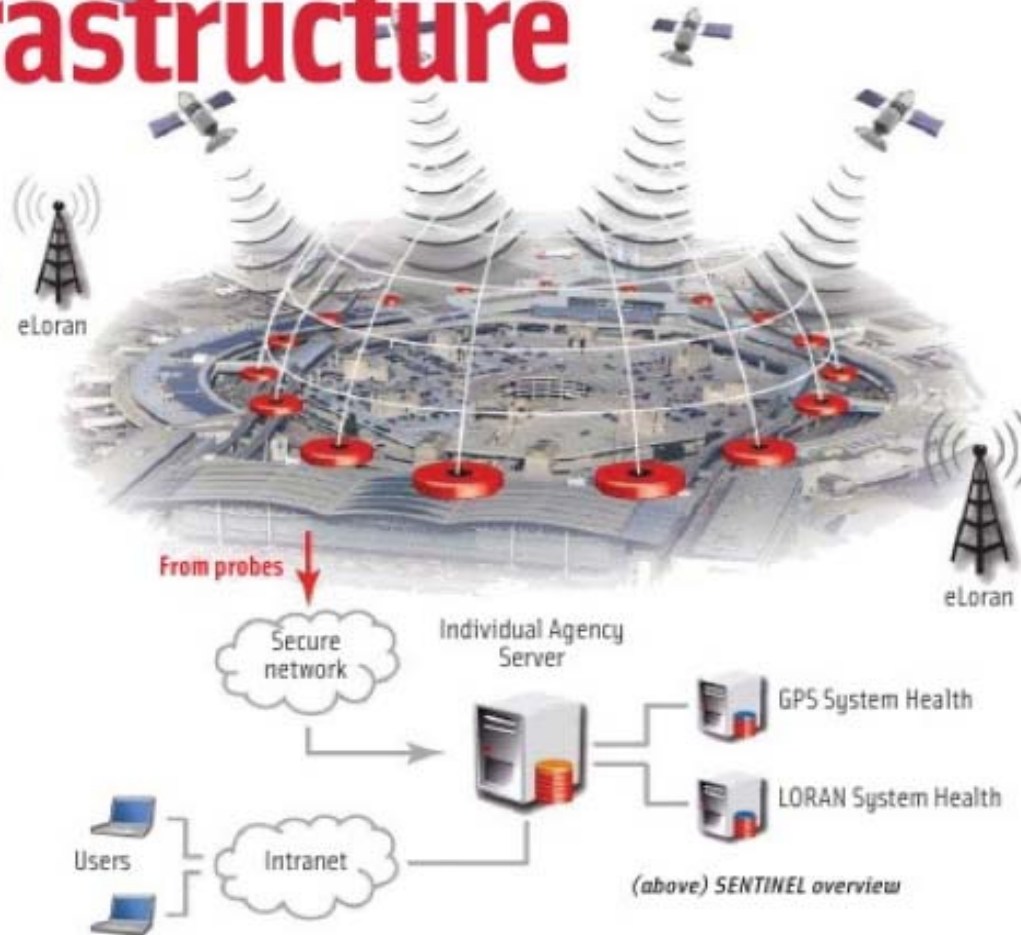
Protecting the UK Infrastructure

A System to Detect GNSS Jamming and Interference

ANDY G. PROCTOR, CHARLES W. T. CURRY
CHRONDS TECHNOLOGY LTD.

JENNA TONG, ROBERT WATSON
UNIVERSITY OF BATH

MARK GREAVES, PAUL CRUDDACE
ORDNANCE SURVEY



Homeland Security

Real time detection & location of GNSS interference for the protection of critical infrastructure facilities and services

White Sands Missile Range Exercise

- Civil Focus, Testing/Training; June 18 – 22
- 1st open air transmission using Commercial Jammers
- Multiple scenarios, moving targets
- Jammer Characterizations
- Training Opportunity
- Patriot Watch Capability Demonstration
- Encourage participant collaboration
- 746th Test Squadron Support



Homeland
Security



Cell Phone

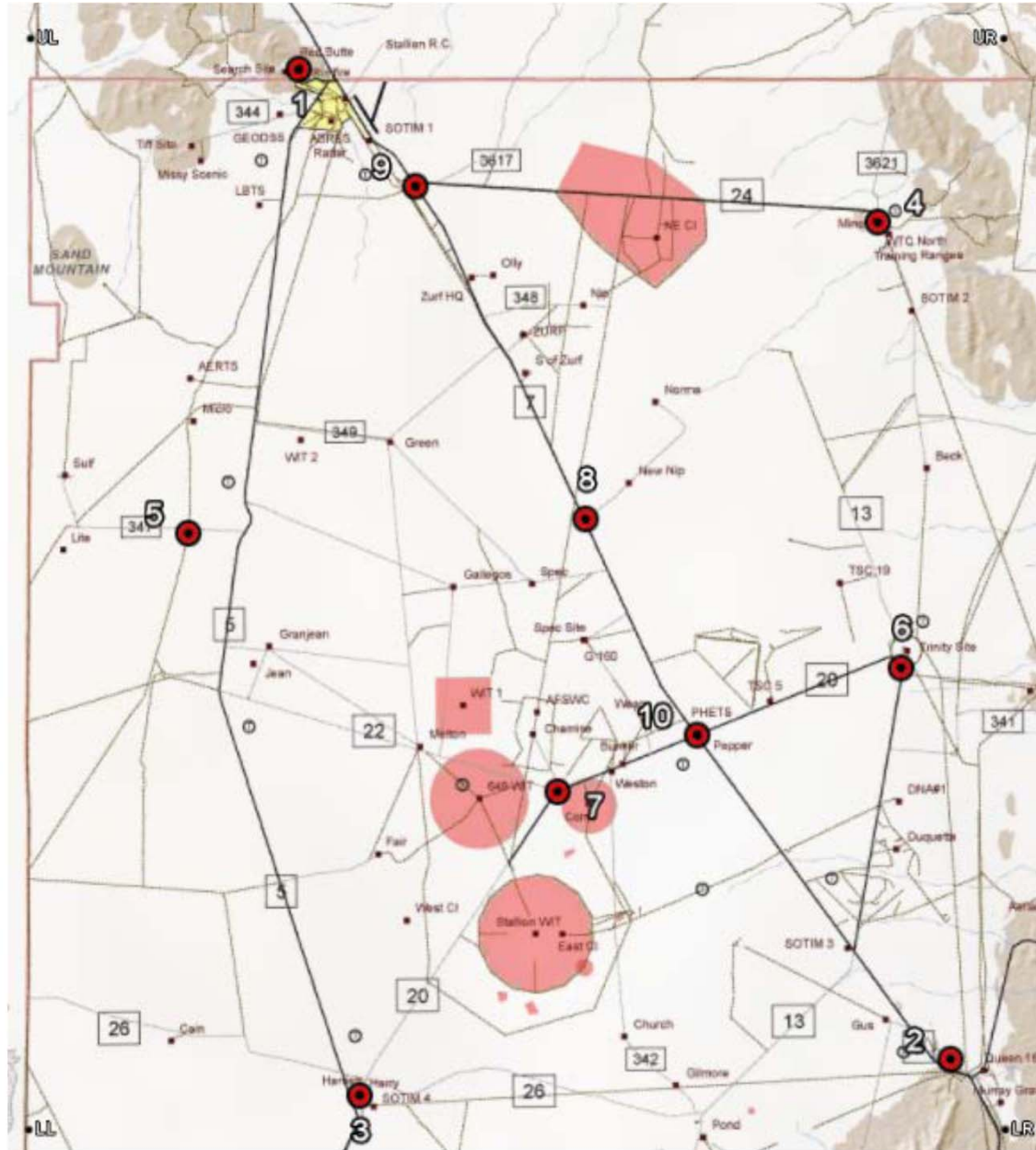
WiFi

GPS

Cell Phone & GPS



Homeland Security



Homeland Security

Mitigation Through Resiliency CIKR Time Backup

- **Distributing the Master Clock on Fiber**
- **Utilize existing fiber infrastructure**
- **Successful prototype NAVFEST February 2011**
 - **USNO Ed Powers and Bill Bollwerk co-sponsors**
- **Long-haul test between USNO Washington DC and Boulder, Colorado/Schriever AFB**
- **Distribution of master clock to specific demarcation**
- **USCG Investigation on use of low frequency for over the air transmission of time**
- **DHS Request For Information January 2012 – ongoing review**



Homeland
Security

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



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**
- **Comprehensive WSMR testing**
- **Research is underway for alternative sources of time**



Homeland
Security

QUESTIONS?

John.Merrill@dhs.gov

202-447-3731

202-731-9628



Homeland
Security