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

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

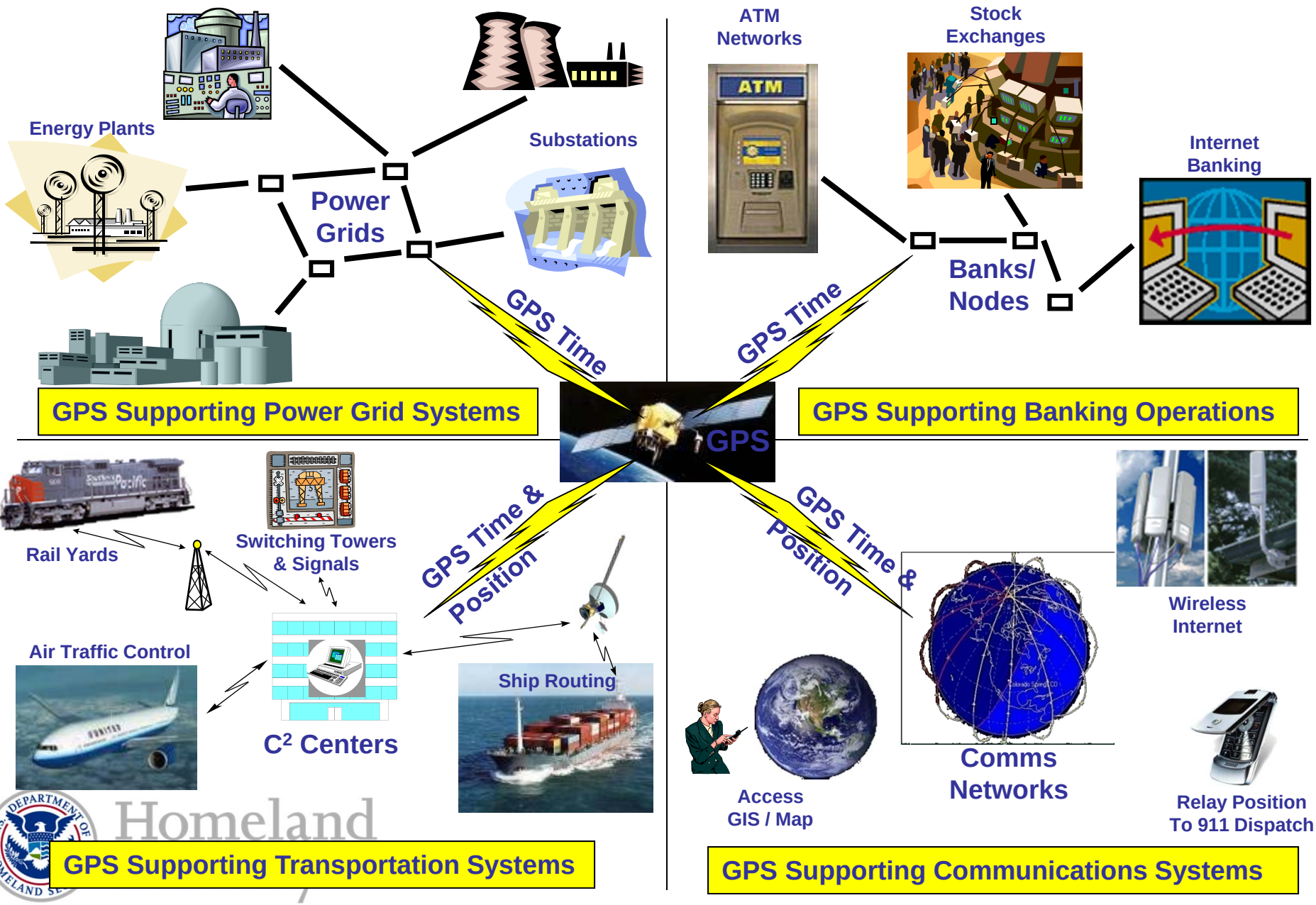

Postal and Shipping

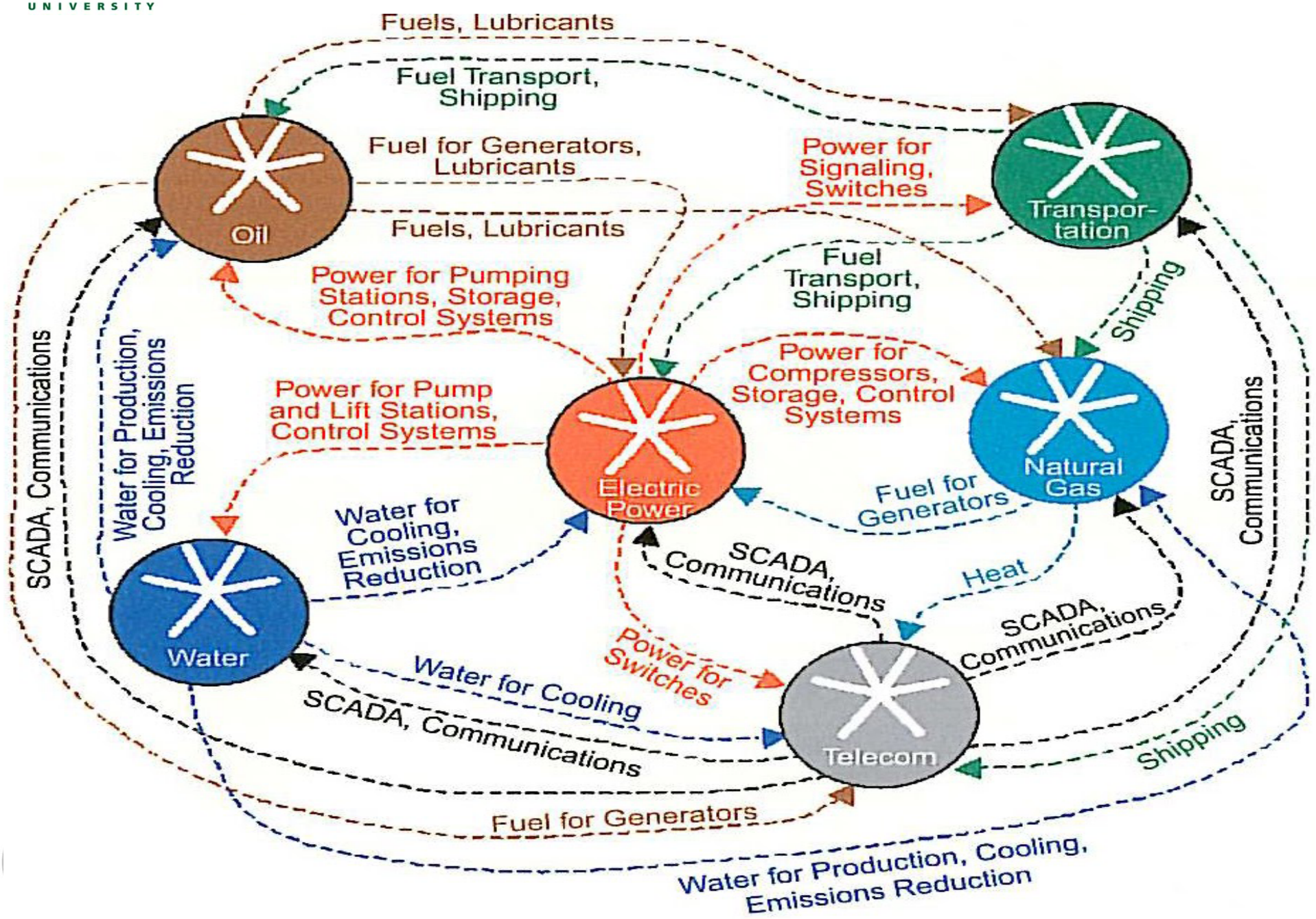

Transportation Systems


Water

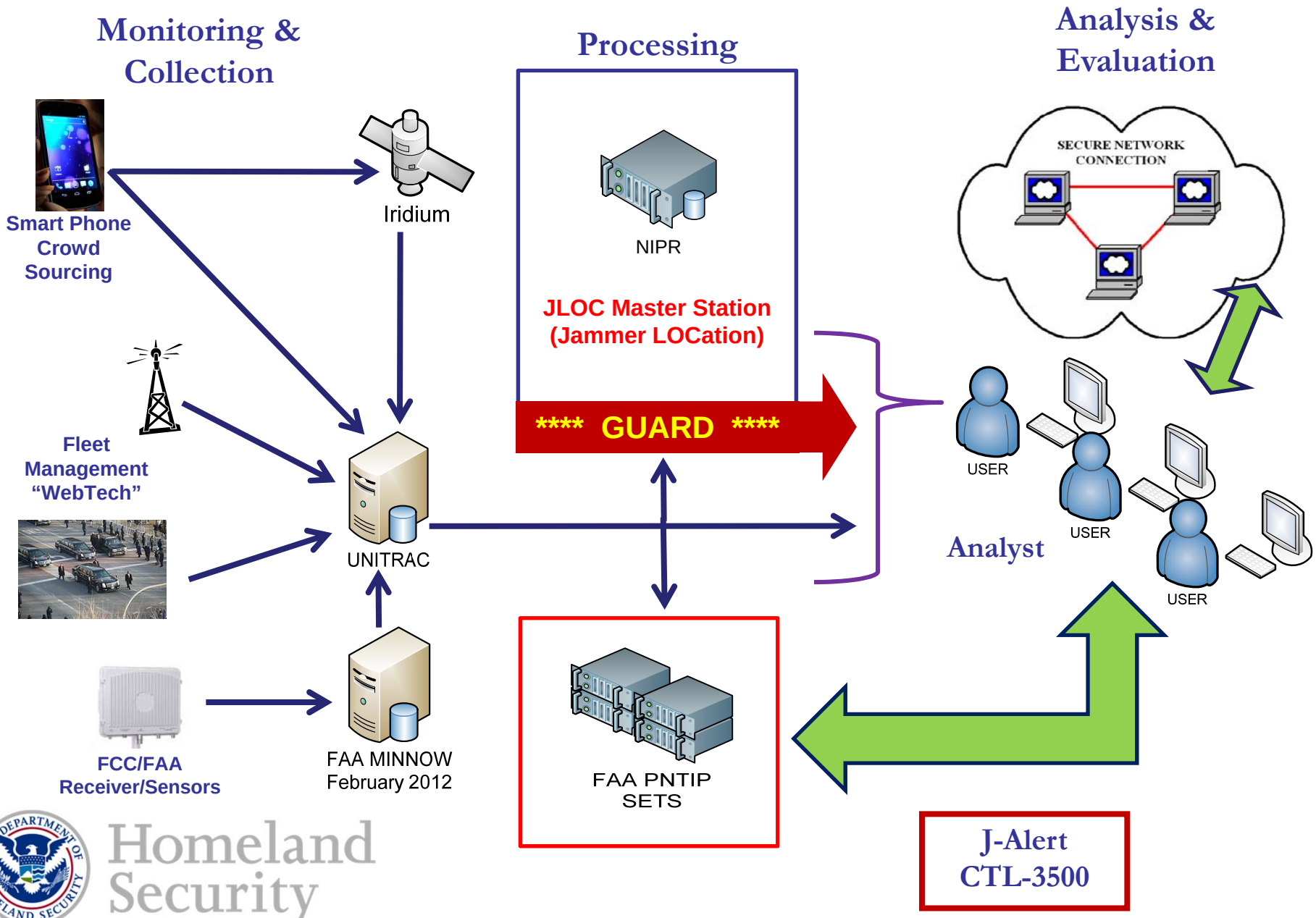
Homeland Security

Extent of GPS Dependencies




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



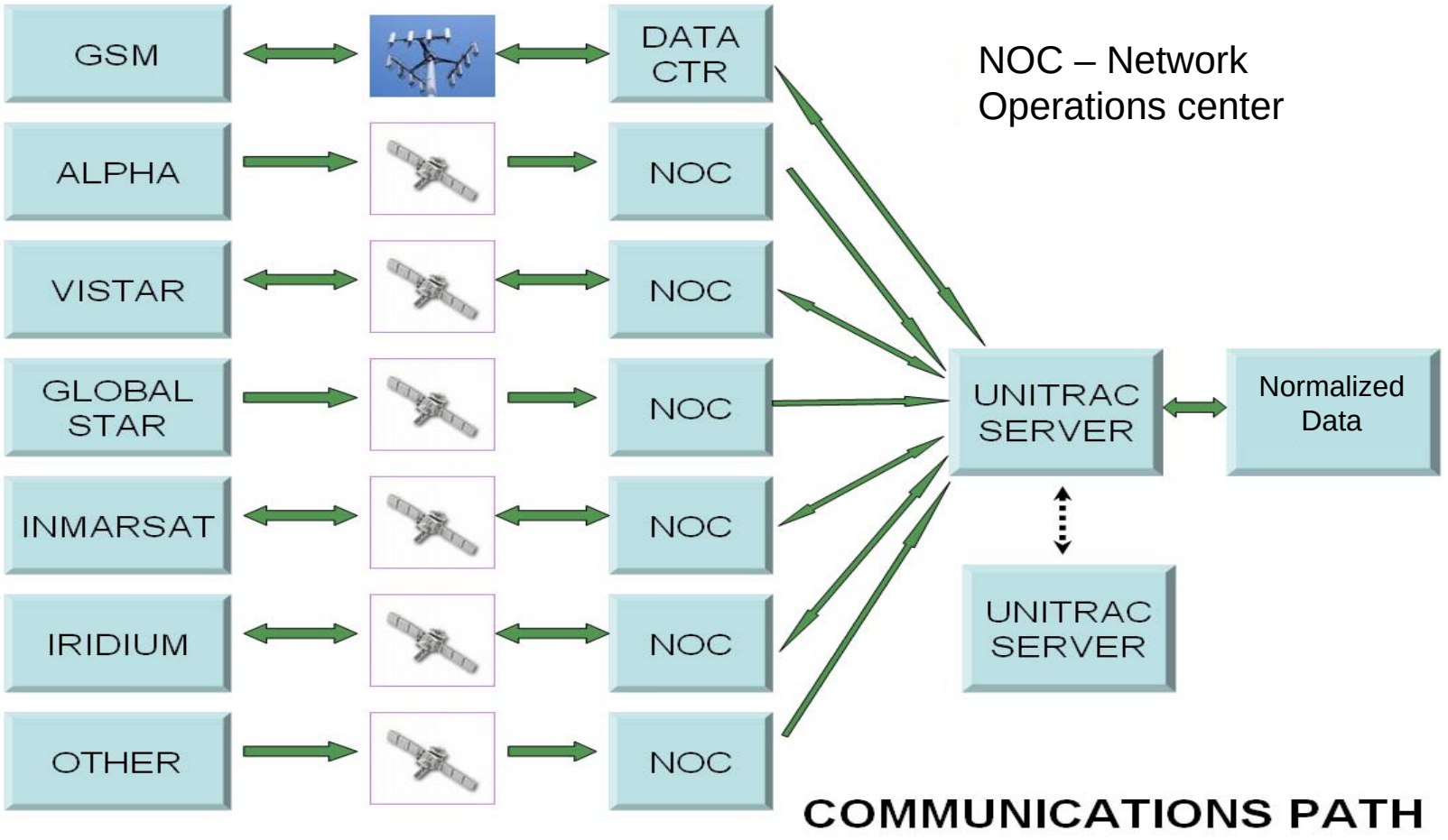
Patriot Watch Standard Data Set

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 fualt, 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 ARCHITECHTURE



Homeland Security

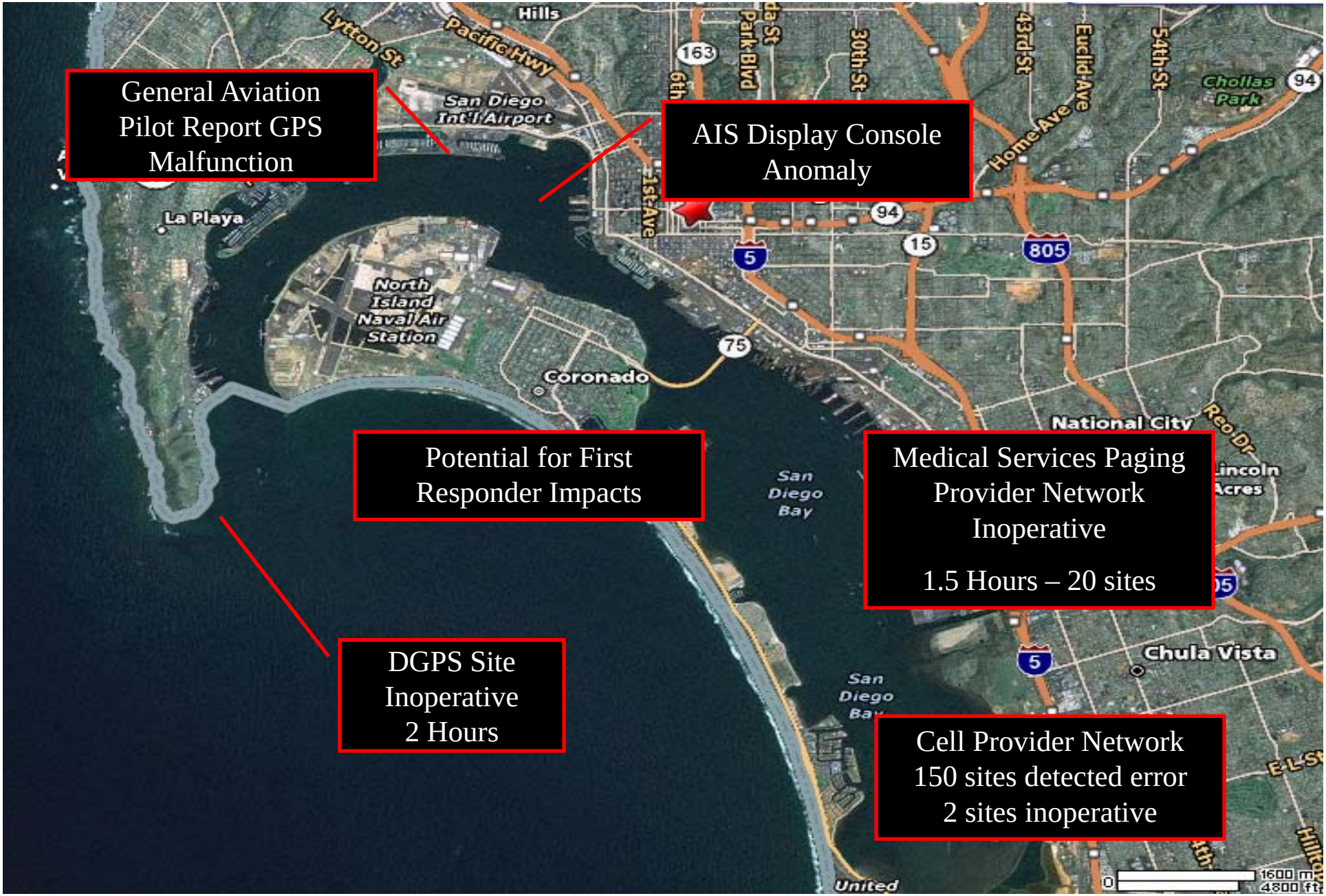
Moss Landing, CA

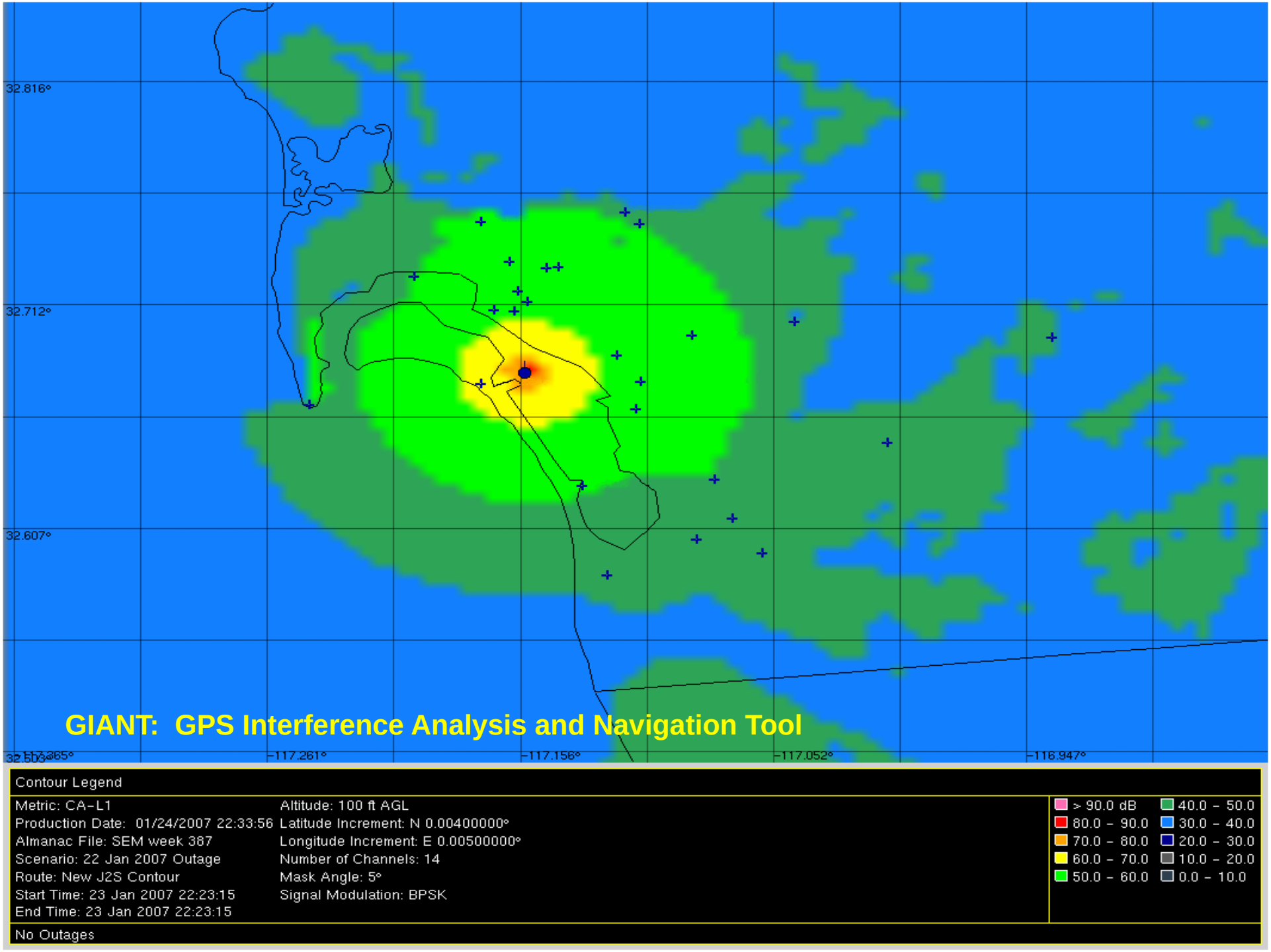
FIGURE 2 search bearing for Source-1

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.

Homeland Security

San Diego January 2007




32.816°
32.712°
32.607°
-117.261°
-117.156°
-117.052°
-116.947°
GIANT: GPS Interference Analysis and Navigation Tool
Contour Legend
Metric: CA-L1
Production Date: 01/24/2007 22:33:56
Almanac File: SEM week 387
Scenario: 22 Jan 2007 Outage
Route: New J2S Contour
Start Time: 23 Jan 2007 22:23:15
End Time: 23 Jan 2007 22:23:15
Altitude: 100 ft AGL
Latitude Increment: N 0.00400000°
Longitude Increment: E 0.00500000°
Number of Channels: 14
Mask Angle: 5°
Signal Modulation: BPSK
> 90.0 dB
80.0 - 90.0
70.0 - 80.0
60.0 - 70.0
50.0 - 60.0
40.0 - 50.0
30.0 - 40.0
20.0 - 30.0
10.0 - 20.0
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

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

VHF Radios (VDB)
- D8PSK modulation, TDMA
- Nav band, 108-118 MHz

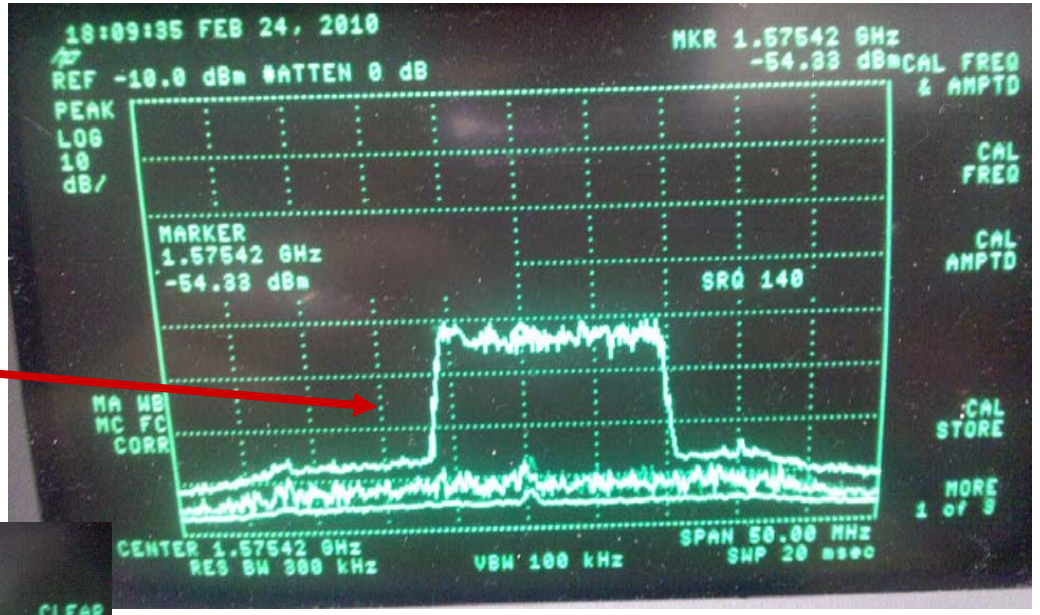
VHF Antenna
- Horizontal (HPOL) or Elliptical (EPOL) polarized signal

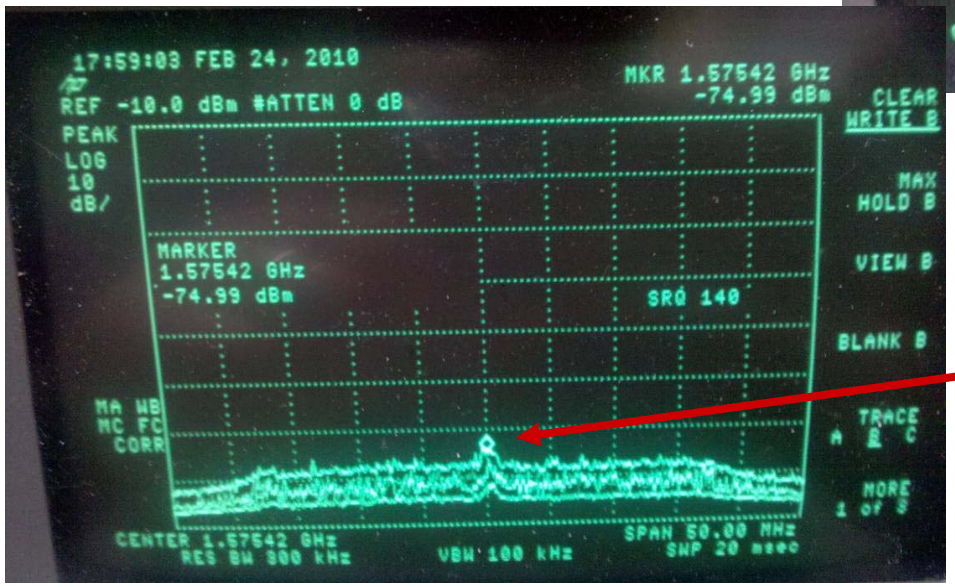
DCP: Differential Correction Processor
RPDP: Robust Power Distribution Panle
VHF: Very High Frequency
VDB: VHF Data Broadcast
HW: Hardware
RRA: Reference Receiver Antenna
RSMU: Remote Satellite Measurement Unit

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.

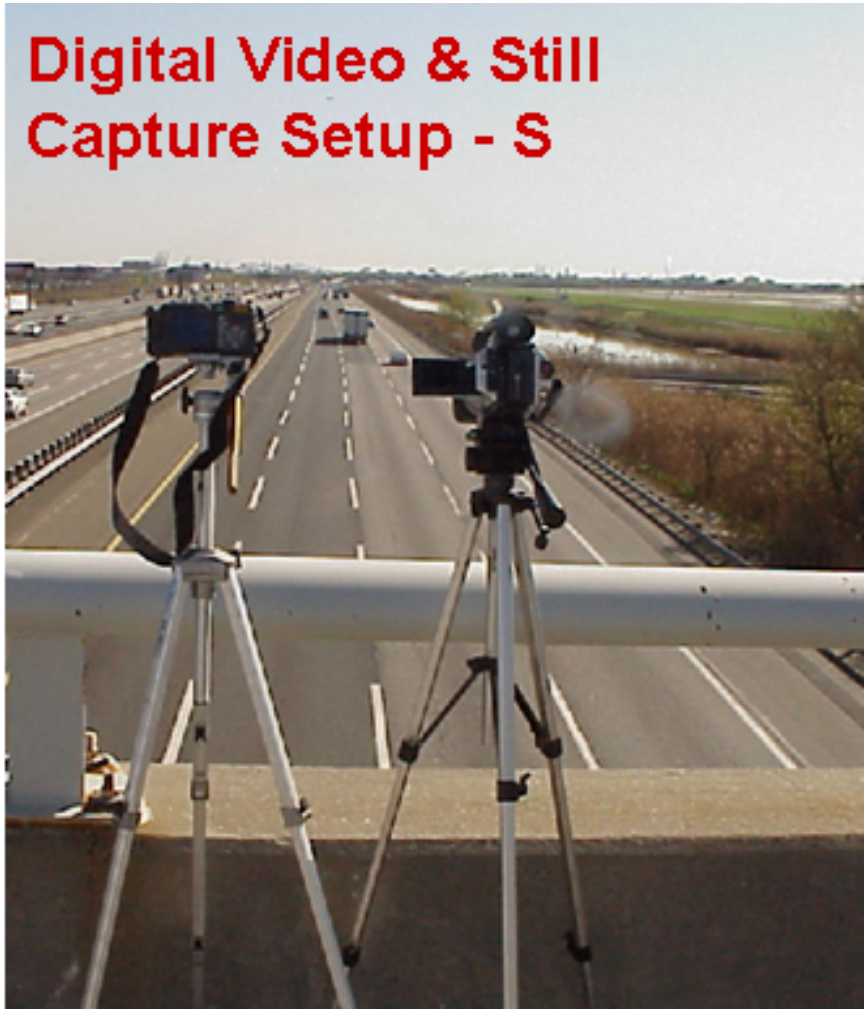
Homeland Security

RFI Source Emission Modeled – Analyze

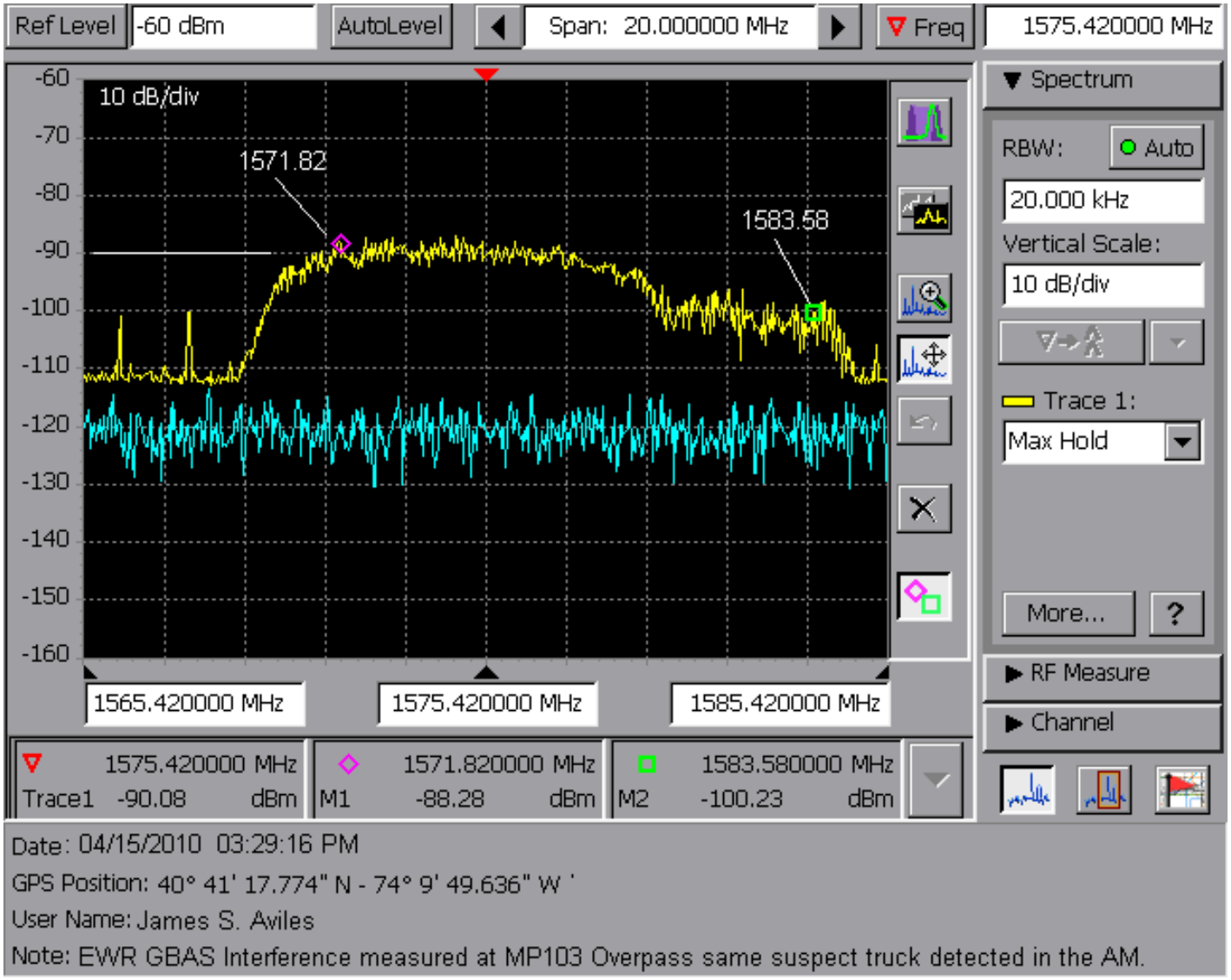
Homeland Security

New Jersey Turnpike Overpass Point – Analyze

Equipment Capture Setup – Analyze

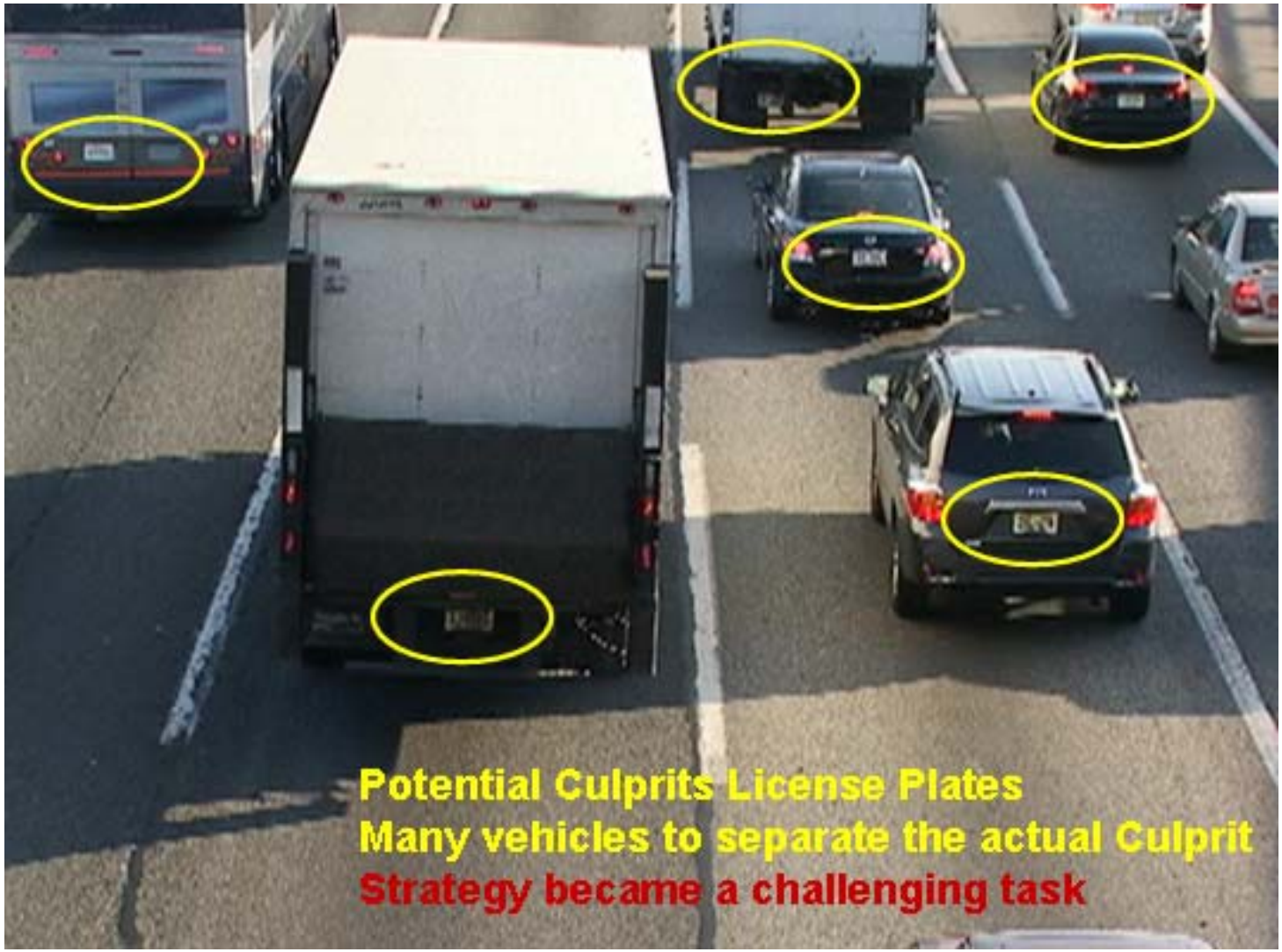


Homeland Security



Homeland Security

… so which one is the culprit?



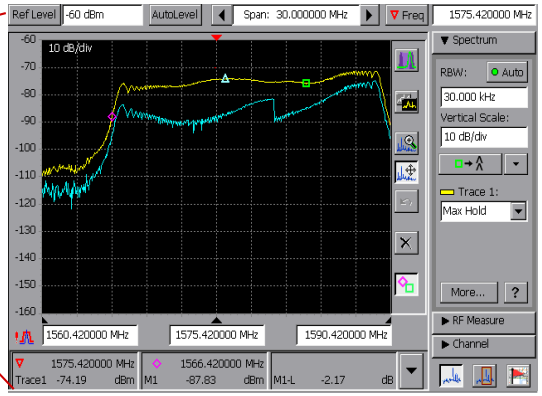
Homeland Security

GPS RFI Source Pursuit – Locate

FCC MDDF Ready

FAA RFHawk Ready

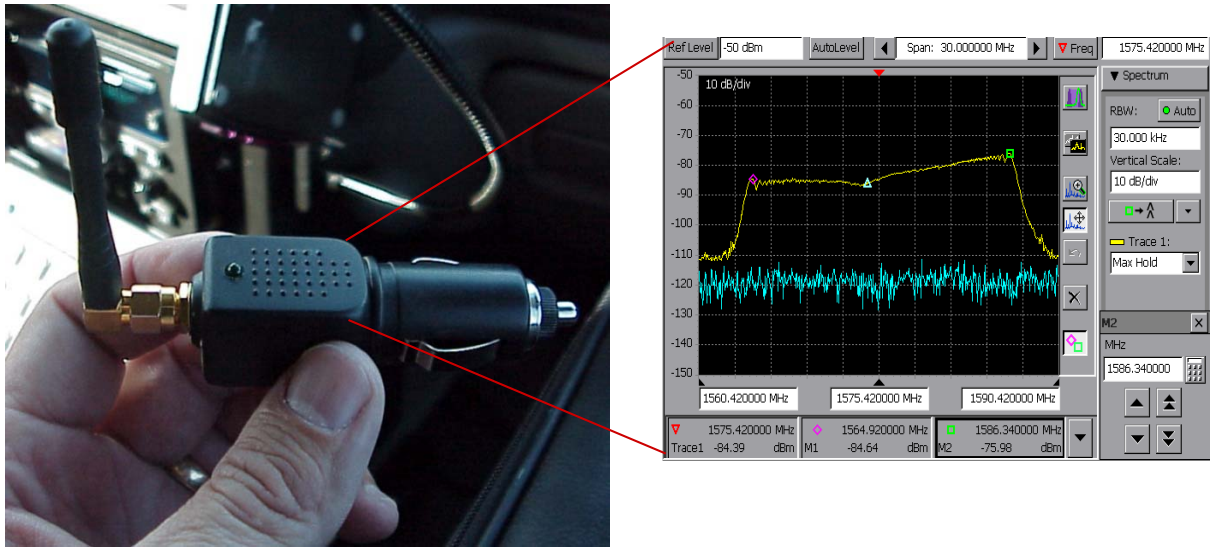
FAA “Tip OFF” Ready



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

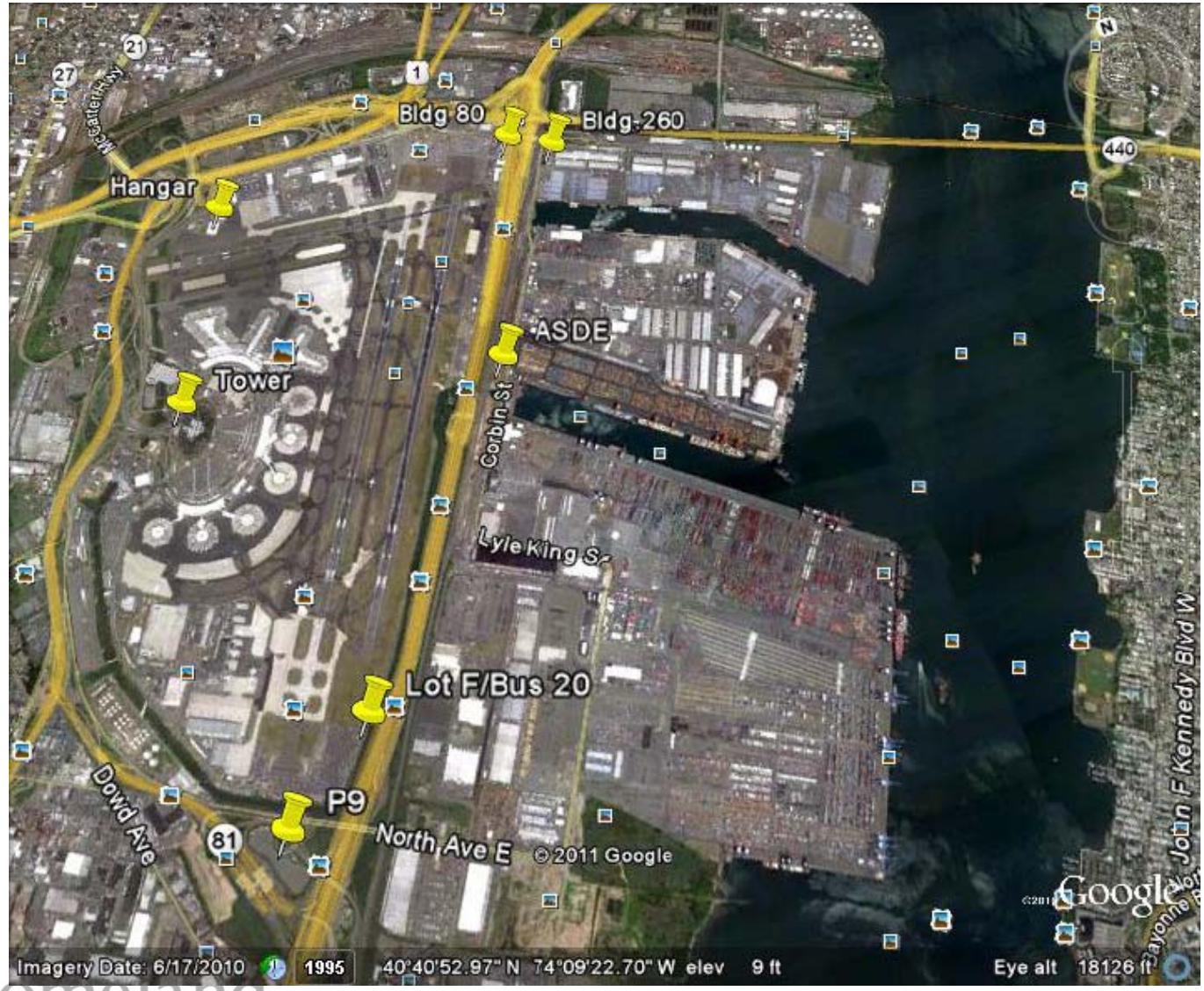


On Site ON-OFF tests confirm surrendered GPS RFI source on April 29, 2010

November 2009 – April 2011 to locate 1 GPS jammer!

Homeland Security

FCC/FAA Minnow Deployment – Locate



Homeland Security

chroma TECHNOLOGY

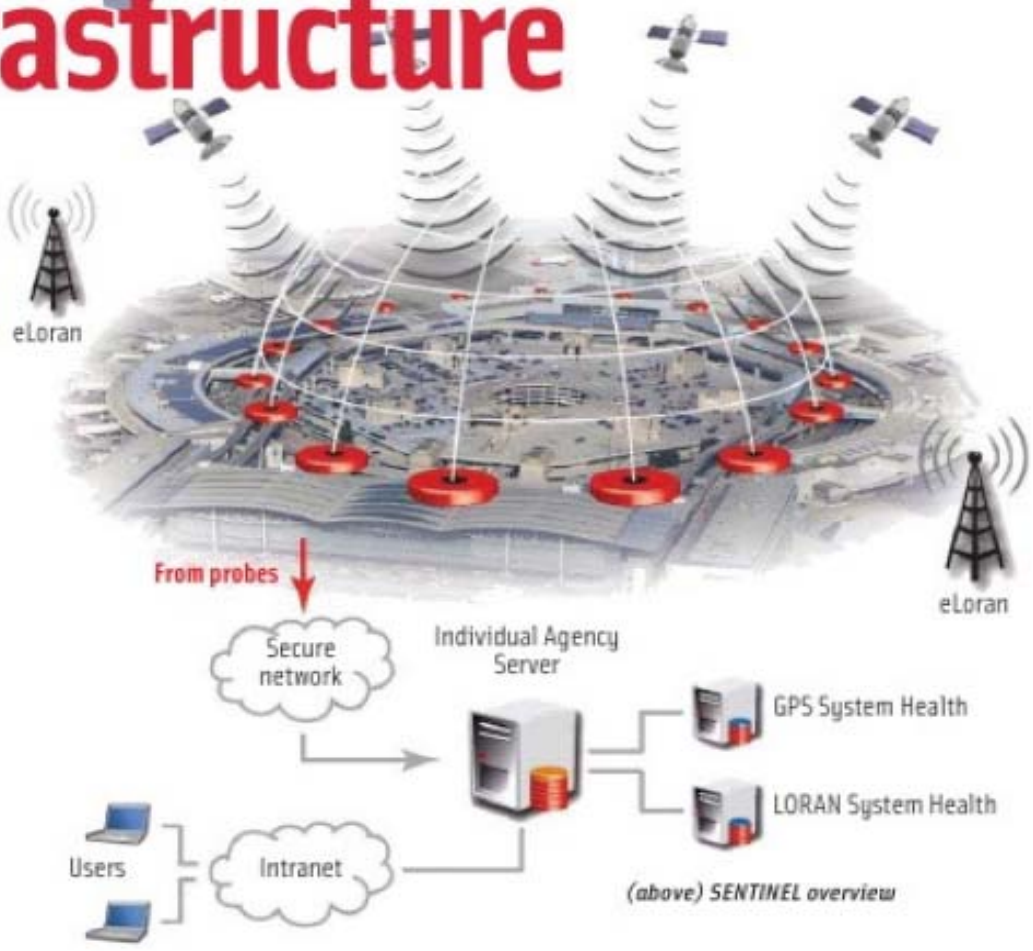
Homeland Security

International Partners Capability

Protecting the UK Infrastructure

A System to Detect GNSS Jamming and Interference

ANDY G. PROCTOR, CHARLES W. T. CURRY
CHRONOS TECHNOLOGY LTD.
JENNA TONG, ROBERT WATSON
UNIVERSITY OF BATH
MARK GREAVES, PAUL CRUDDACE
ORDNANCE SURVEY



Homeland Security

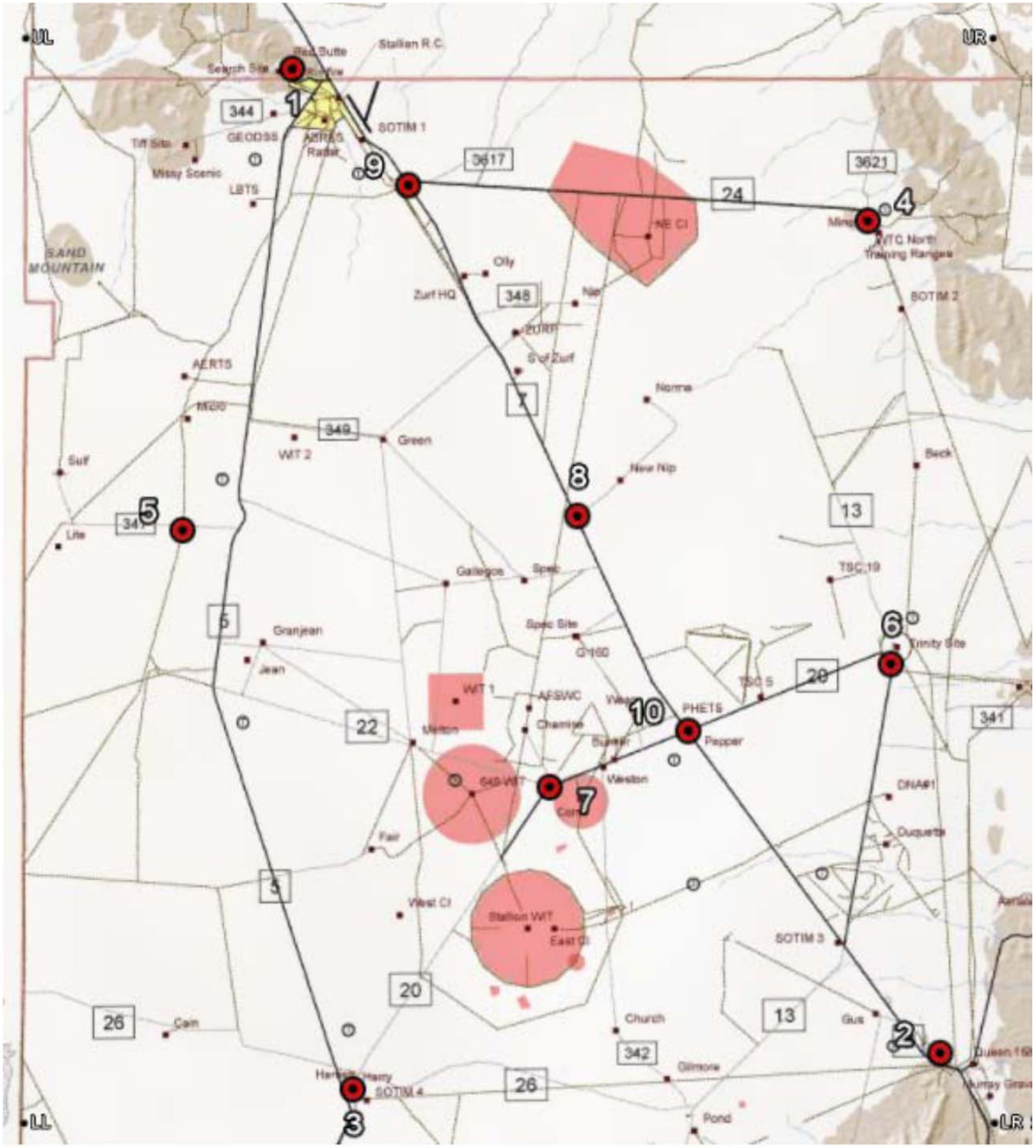
Real time detection & location of GNSS interference for the protection of critical infrastructure facilities and services

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

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

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