

UNCLASSIFIED

United States GPS Interference Detection and Mitigation (IDM)

Rick Hamilton

GPS Information Analysis
U.S. Coast Guard Navigation Center

John Merrill

DHS PNT Program Manager
Office of Applied Technology Geospatial Management Office



Homeland
Security

UNCLASSIFIED

U.S. Department of
Homeland Security
**United States
Coast Guard**



Topics of Discussion

- **Governance**
- **Existing/Emerging Threats Assessments**
- **Patriot Watch – A National Capability**
 - **Critical Infrastructure Key Resources**
 - **CONOPS Development**
 - **PNT Incident Portal/Central Data Repository**
 - **National Sensor Capability initiatives**



US DHS IDM Mandates

- **Collect, analyze, store, & disseminate interference reports from all sources to enable appropriate investigation, notification & enforcement action.**
- **Coordinate United States domestic capabilities to identify, analyze, locate, attribute, & mitigate sources of interference to GPS & its augmentations systems.**
- **Develop & maintain capabilities, procedures & techniques, & routinely exercise civil contingency responses to ensure continuity of operations in the event that access to GPS signal is disrupted or denied.**



US DHS IDM Initiatives

- **DATA**: Collect, analyze, store, & disseminate interference incidents from all reporting sources
- **TOOLS**: Coordinate US domestic capabilities to identify, analyze, locate, attribute, & mitigate sources of interference to the GPS & its augmentations
- **ACTION**: Develop & maintain capabilities, procedures & techniques, & routinely exercise civil contingency responses to ensure continuity of operations in the event that access to GPS signal is disrupted or denied



Existing/Emerging Global Threats



GPS and GSM Jammer



U.K. £150



1 Watt Jammer

Links between Criminal & Terrorist activity are indisputable

GPS Navigation Devices Can Be Duped

By Scott Branson
Special to GPS World.com
Just like flat-screen televisions, cell phones and computers, global positioning system (GPS) technology is becoming something people can't imagine living without. So if such a ubiquitous system were to come under attack, would we be ready?



Tim Himmelsp, right, discusses with Paul Varney, left, and Matt Pickett how a GPS receiver can be "spoofed," based on the research of Paul A. Cornell, Robert Kane/US Army Research Laboratory

It's an uncomfortable question, but one that a group of Cornell researchers have considered with their research into "spoofing" GPS receivers.

GPS is a U.S. navigation system of more than 30 satellites circling Earth twice a day in specific orbits, transmitting signals to receivers on land, sea and in air to calculate their exact locations. "Spoofing," a non-secure technical term first coined in the radar community, is the transmission of fake GPS signals that receivers accept as authentic ones.

The Washington Post

Guns Used Technology as A Tactical Tool
Hacker Proves That GPS Laps Satellite Uses

Haste Could Make Waste

Obama Teams Are Scrutinizing

Coaxing!

Aug 08, FCC cites Colorado business for selling GPS jammers to counter GPS vehicle trackers

Police Turn to Secret Weapon: GPS Device

By Lisa Himmelsp
Washington Post Staff Writer

Someone was attacking women in Fairfax County and Alexandria, grabbing them from behind and sometimes punching and molesting them before running away. After logging 11 cases in six months, police finally identified a suspect.

David Lee Kelly Jr., who had served 12 years in prison for rape, lived near the crime scenes. To figure out if Kelly was the assailant, police pulled out their secret weapon: They put a Global Positioning System device on Kelly's car, which allowed them to track his movements.

Police said they soon caught Kelly dragging a woman into a wooded

area in Falls Church. After his arrest on Feb. 5, the string of assaults suddenly stopped. The break in the case relied largely on a crime-fighting tool they would rather not discuss.

"We don't really want to give our info on how we use it as an investigative tool to help the bad guys," said Officer Shelley Boudrie, a Fairfax police spokesman. "It is an investigative tool for us, and it is every non-investigative tool."

Across the country, police are using GPS devices to snare thieves, drug dealers, sex-off predators and killers, often without a warrant or court order. Privacy advocates and tracking respects electronically

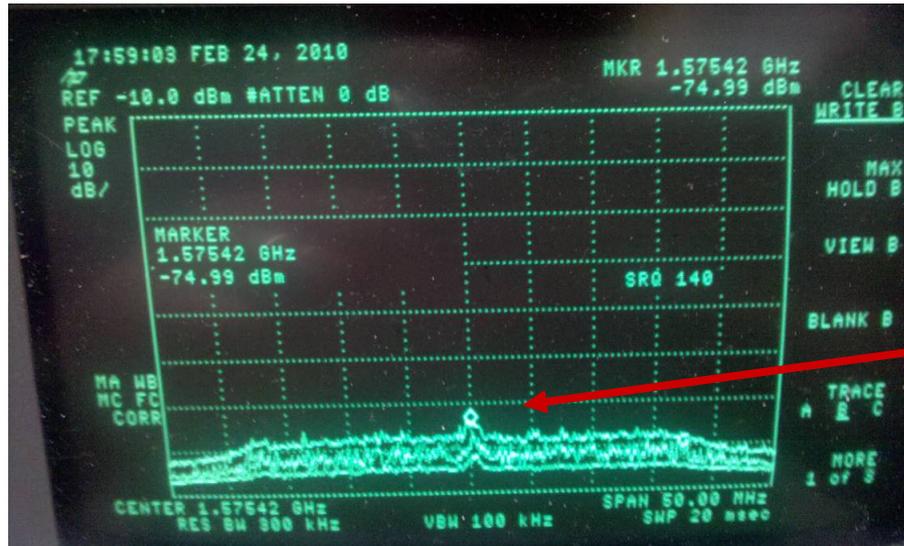
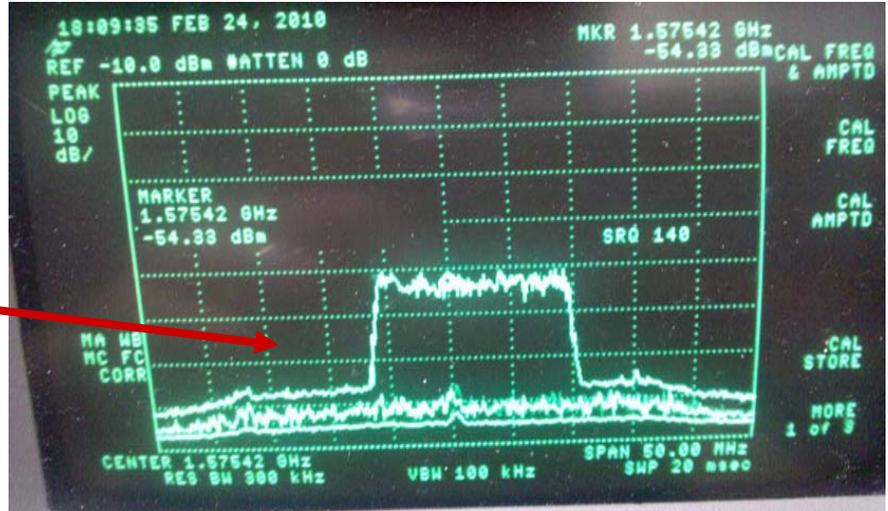
See GPS DEVICES, A12, C1, 1



Homeland Security

US Government Measurements

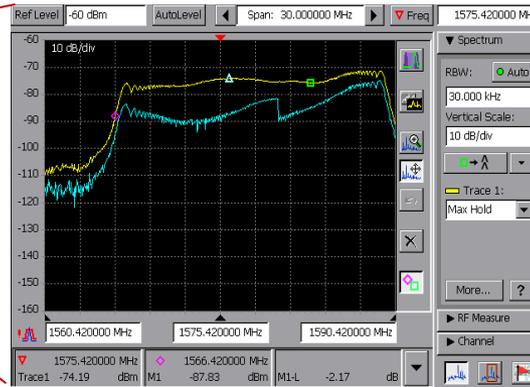
Wideband RFI Source measured occupying approximately 20 MHz – 5 MHz below L1 and 15 MHz above L1.



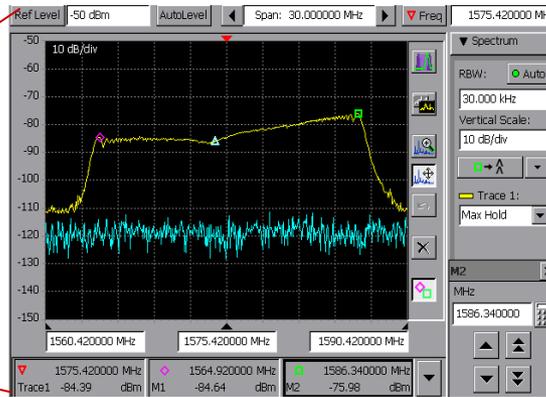
Normal L1 passband Spectrum when RFI Source is not present.



US Government Finding



**RFI source
“Locked-on” and
pursued.**



**On Site ON-OFF
tests confirms
GPS RFI source.**

Regulations in the U.S.

U.S. Federal statutes and regulations generally prohibit the manufacture, importation, sale, advertisement, or shipment of devices, such as jammers, that fail to comply with FCC regulations.

Regulations in the U.S.

U.S. Federal Statutes – Communications Act

- 47 U.S.C. § 301 Unlicensed (unauthorized) operation prohibited
- 47 U.S.C. § 333 – Interference to authorized communications prohibited
- 47 U.S.C. § 302a(b) Manufacturing, importing, selling, offer for sale, shipment or use of devices which do not comply with regulations are prohibited

Regulations in the U.S.

Telecom Agency Rules - FCC

- 47 C.F.R. § 2.803(a) - marketing is prohibited unless devices are authorized and comply with all applicable administrative, technical, labeling and identification requirements.
- 47 C.F.R. § 2.803(e)(4) - marketing is defined as “sale or lease, or offering for sale or lease, including advertising for sale or lease, or importation, shipment, or distribution for the purpose of selling or leasing or offering for sale or lease.”



US CONOPS Development

- **Critical Infrastructure Key Resources (CIKR) Study:**
 - Dependency on GPS
 - Impacts and Priorities
 - Tools to Mitigate Vulnerability Gaps
 - Tests on Vulnerabilities – To Measure Effective Mitigation Tools
- **US Government Command Post Exercises**
 - Exercise Interagency checklist with clear lead, supporting authorities and incident ranking criteria
 - Exercise Multi-agency collaborative environment for shared situational awareness
 - Further Exercises w/greater complexity, scope, & interaction with extended government capabilities
- **Draft early 2011**



CIKR Sectors



[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](#)



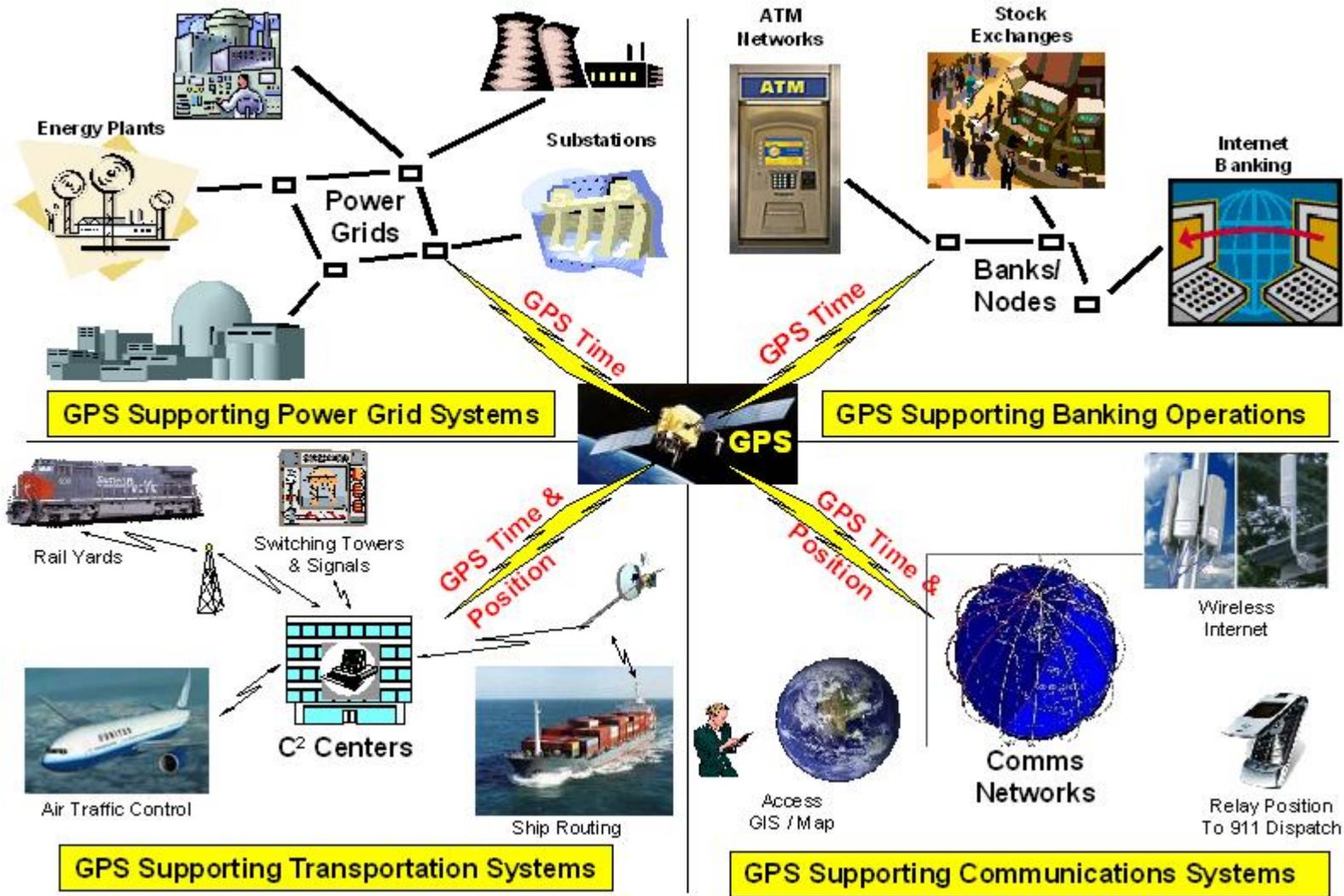
[Transportation Systems](#)



[Water](#)

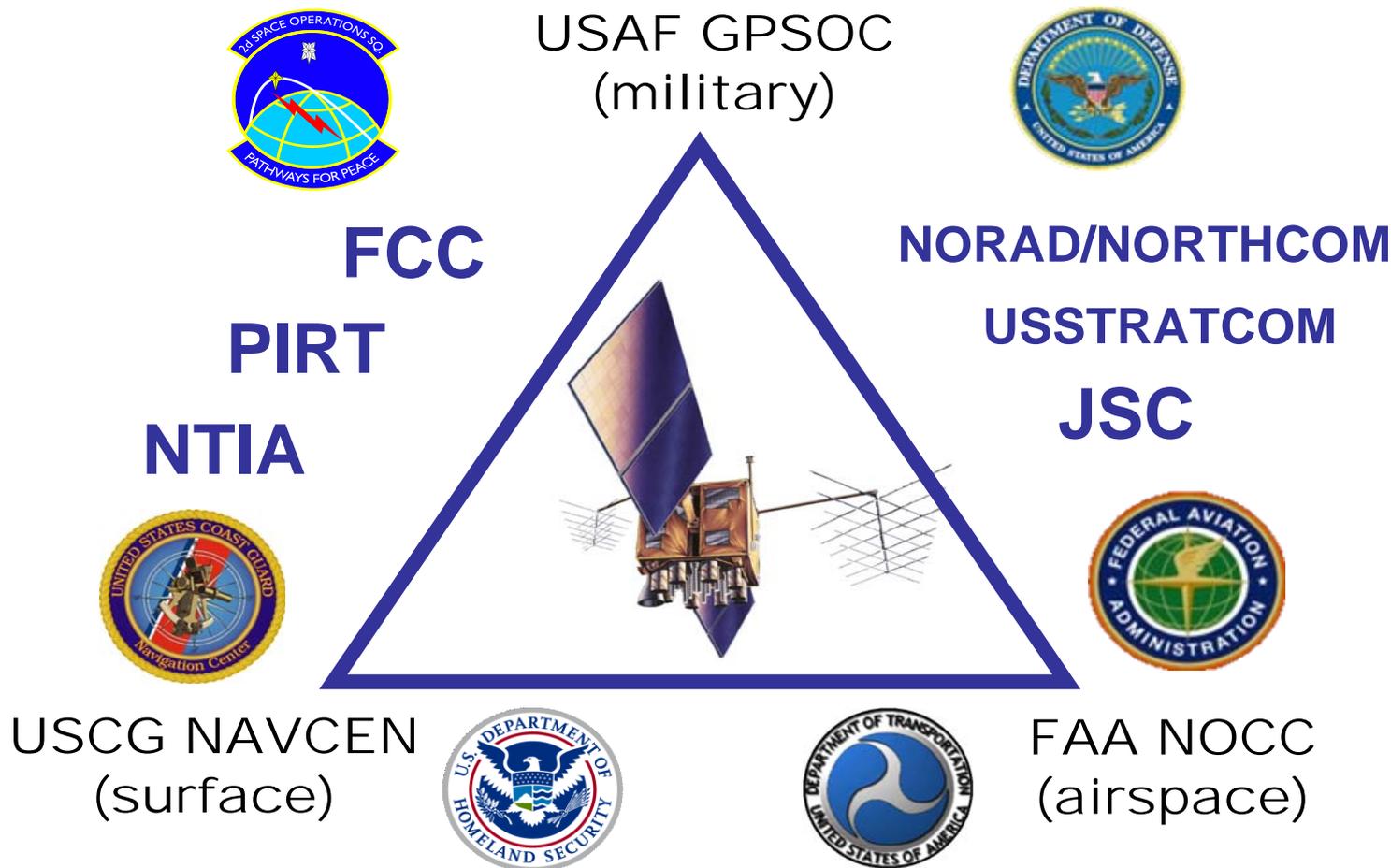


Extent of GPS Dependencies



The GPS Triad

Joint GPS User Support Service



Patriot Watch Customer Base/Users



Homeland Security

U.S. Department of Homeland Security
United States Coast Guard



GPS Civil Performance

- The TRIAD uses DOD developed tools to predict GPS performance impacts due to satellite constellation status
- Enables prediction of Horizontal Dilution of Precision (HDOP); measure of surface user accuracy.
- HDOP out of tolerance (more than 6) triggers a coordinated regional user notification (Notice to Airman (NOTAM) or Notice to Mariners (NTM)).

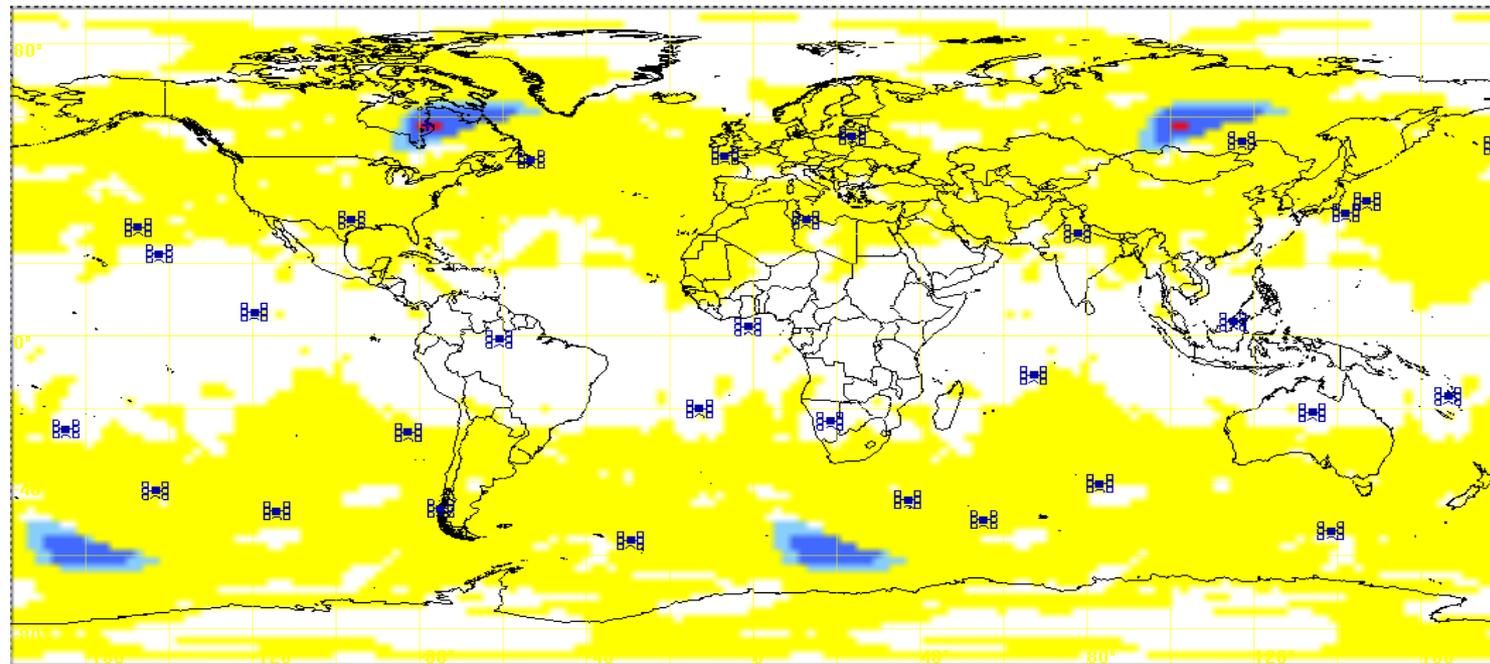




NAVCEN DAILY SYSTEMS BRIEF

Prediction
16 AUG 2010

GPS HDOP



Contour Legend

Metric: HDOP Max	Scenario: 16AUG10	Latitude Increment: 02° 00'	> 12.0	0.0 - 2.0
Production Date: 08/15/2010 20:44:44	Route: World - 4 channels	Longitude Increment: 002° 00'	9.0 - 12.0	
Almanac File: 227.AL3	Start Time: 16 Aug 2010 00:00:00Z	Number of Channels: 4	6.0 - 9.0	
SOF File: 2010_225_214929_v02	End Time: 16 Aug 2010 23:59:00Z	Mask Angle: 5°	4.0 - 6.0	
PSF File: N/A	Altitude: 0 ft HAE	Signal Modulation: BPSK	2.0 - 4.0	

PRN: 25 Outage: 28 May 2010 03:00:00 to Until Further Notice

UNCLASSIFIED

UNCLASSIFIED



Homeland Security

UNCLASSIFIED

U.S. Department of
Homeland Security
**United States
Coast Guard**



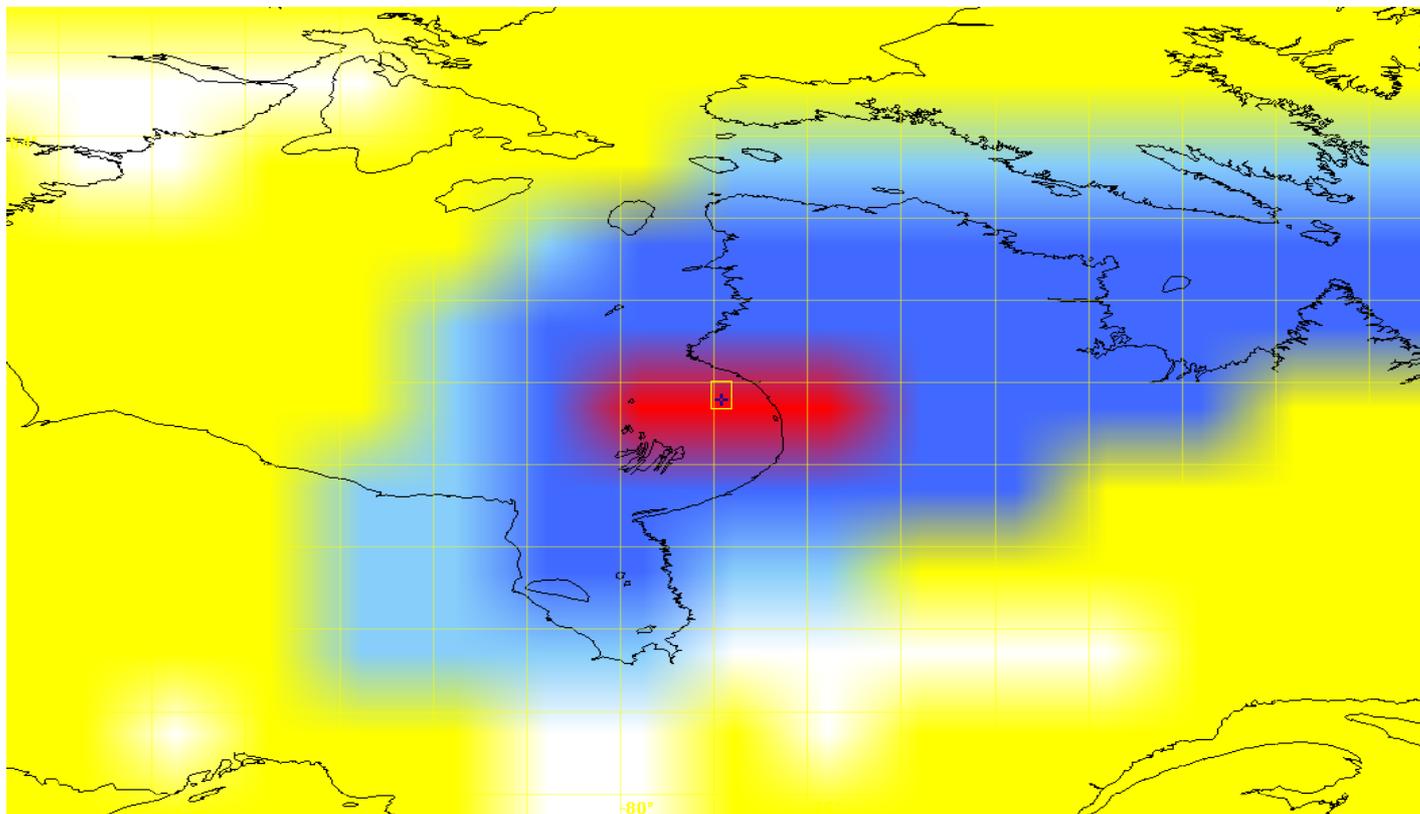


NAVCEN DAILY SYSTEMS BRIEF

GPS HDOP

Prediction

16 AUG 2010



Contour Legend

Metric: HDOP Max	Scenario: 16AUG10	Latitude Increment: 02° 00'	> 12.0	0.0 - 2.0
Production Date: 08/15/2010 20:44:44	Route: World - 4 channels	Longitude Increment: 002° 00'	9.0 - 12.0	
Almanac File: 227.AL3	Start Time: 16 Aug 2010 00:00:00Z	Number of Channels: 4	6.0 - 9.0	
SOF File: 2010_225_214929_v02	End Time: 16 Aug 2010 23:59:00Z	Mask Angle: 5°	4.0 - 6.0	
PSF File: N/A	Altitude: 0 ft HAE	Signal Modulation: BPSK	2.0 - 4.0	

PRN: 25 Outage: 28 May 2010 03:00:00 to Until Further Notice

UNCLASSIFIED

UNCLASSIFIED

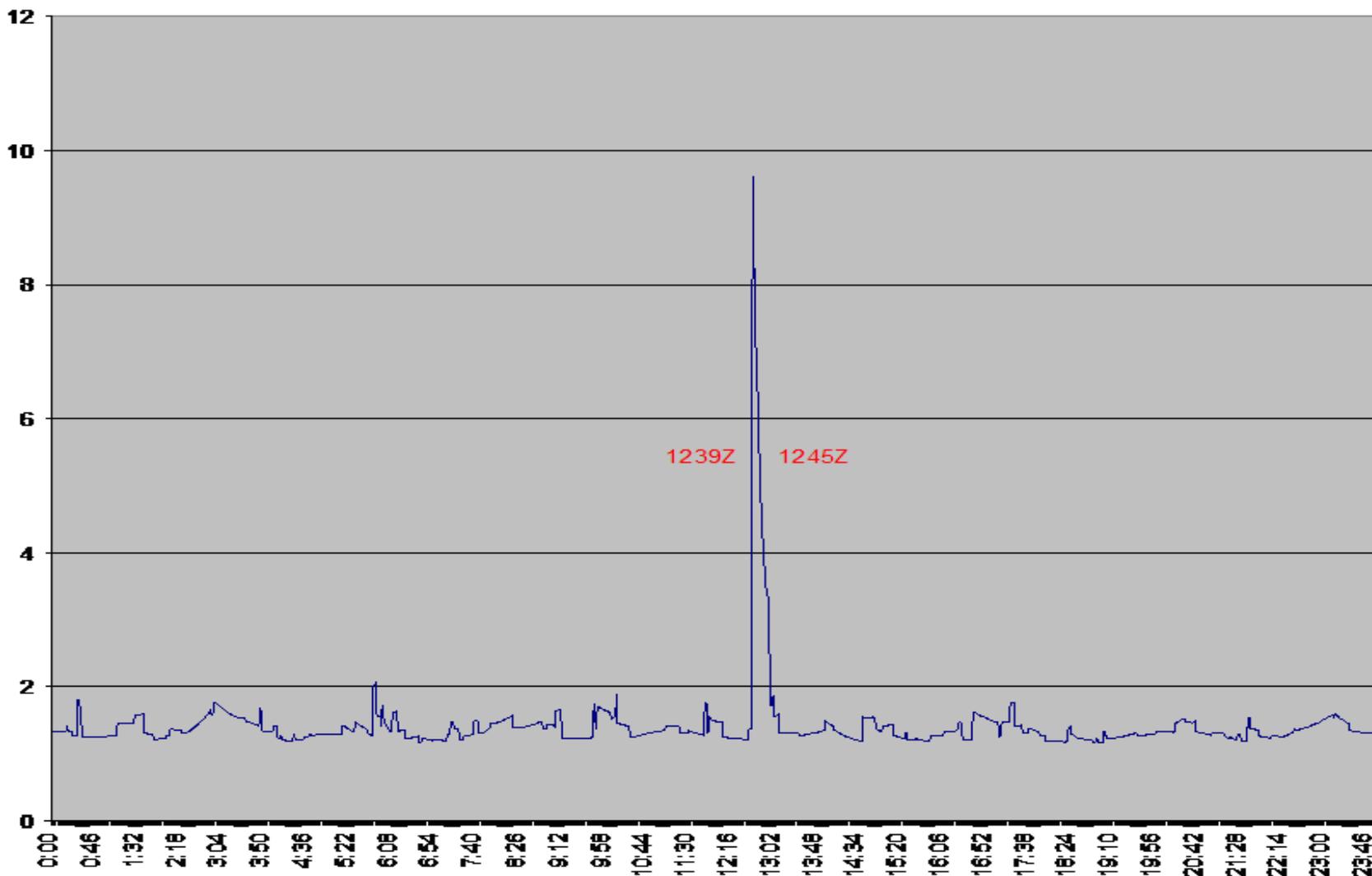


Homeland Security



UNCLASSIFIED

Hudson Bay



Homeland Security

UNCLASSIFIED

U.S. Department of Homeland Security
United States Coast Guard



Central Data Repository Requirements

(Policy Derived Qualitative)

- **Central Interference Reporting database for all PNT incidents**
- **Encompass process and functions for detection validation, investigation, assessment, corroboration of PNT incidents**
- **Automated dissemination of data and reduce PNT incidents information distribution delays for decision support**
- **Mechanisms for cataloging PNT applications and associated vulnerabilities to interference**
- **Employ information assurance components and processes to protect database**
- **Assure the integrity of PNT incidents and sensors**



Secure User Authentication

PNTIP - > Login



Login Email:

Password:

[Change Password?](#) | [Lost Password?](#)

For Account information, contact your respective
[Sys Admin](#)

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.



Homeland
Security

U.S. Department of
Homeland Security
**United States
Coast Guard**



20

Central Data Repository

- **Baseline Requirements – Cost control, use existing architecture**
- **Designed Leverage – Modeled based on the FAA Spectrum Engineering Tracking System (SETS)**
- **Visual Operational Picture – Integrated Common Analytical Viewer (iCAV)**
 - **Geospatial enabling/visualization tool**
 - **Integrates multiple geospatial data sources from a centralized geospatial data warehouse**
 - **Based on the Environmental Systems Research Institute's (ESRI) suite of products.**





Search

Help

Clear Graphics

Bookmarks

e.g., 4600 Sangamore Rd, Bethesda, Md or Statue of Liberty

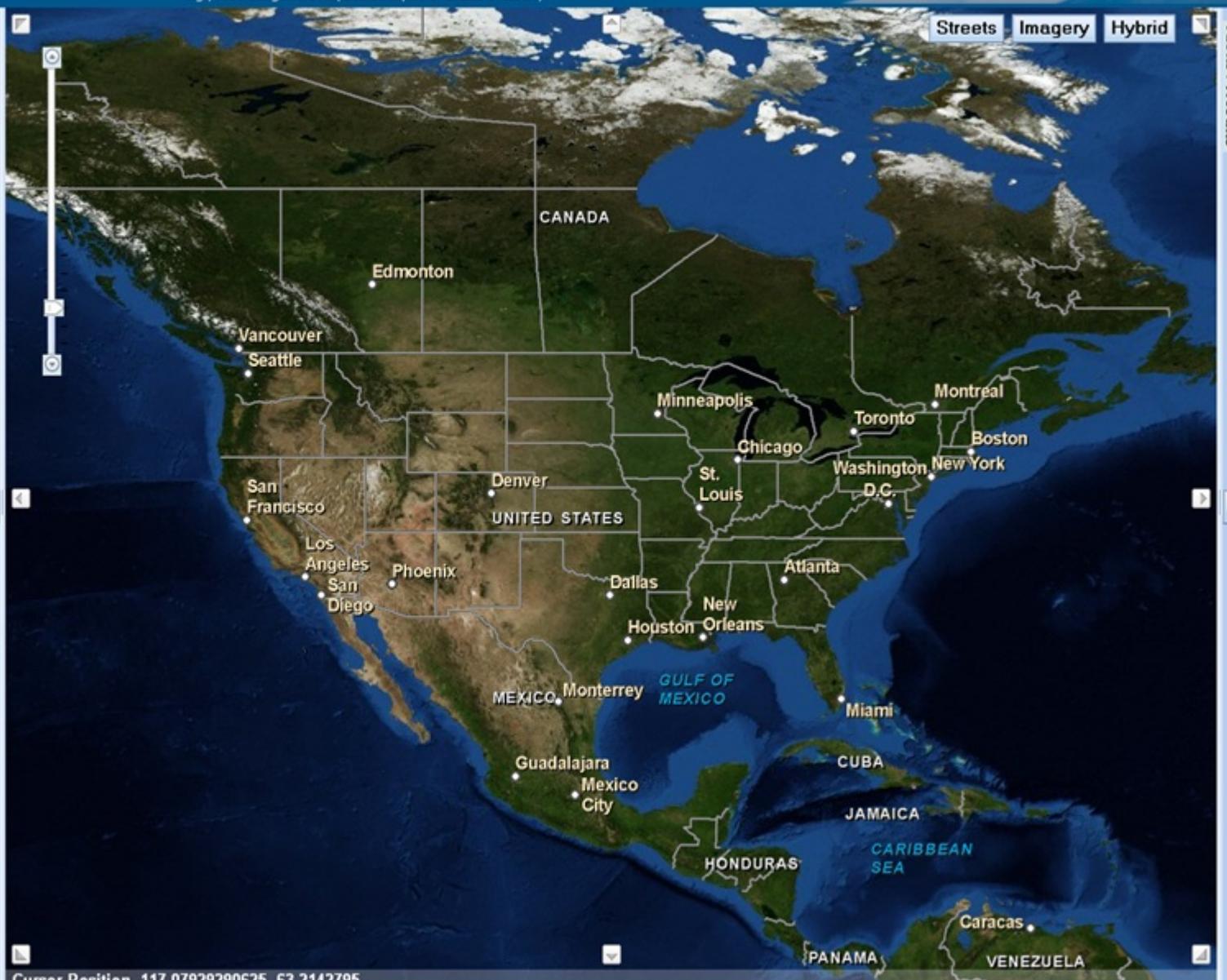
Streets Imagery Hybrid

Tasks / Results

Overlays

- Hurricane Content
- 2008 Midwest Flooding
- NGA Content
- DHS Themes
- HSIP Overlays

- Weather Content
- Imagery Overlays



Cursor Position -117.07929290625, 63.2142795

SAN DIEGO COUNTY

GCS North American 1983
Datum: D North American 1983

 Source of Interference



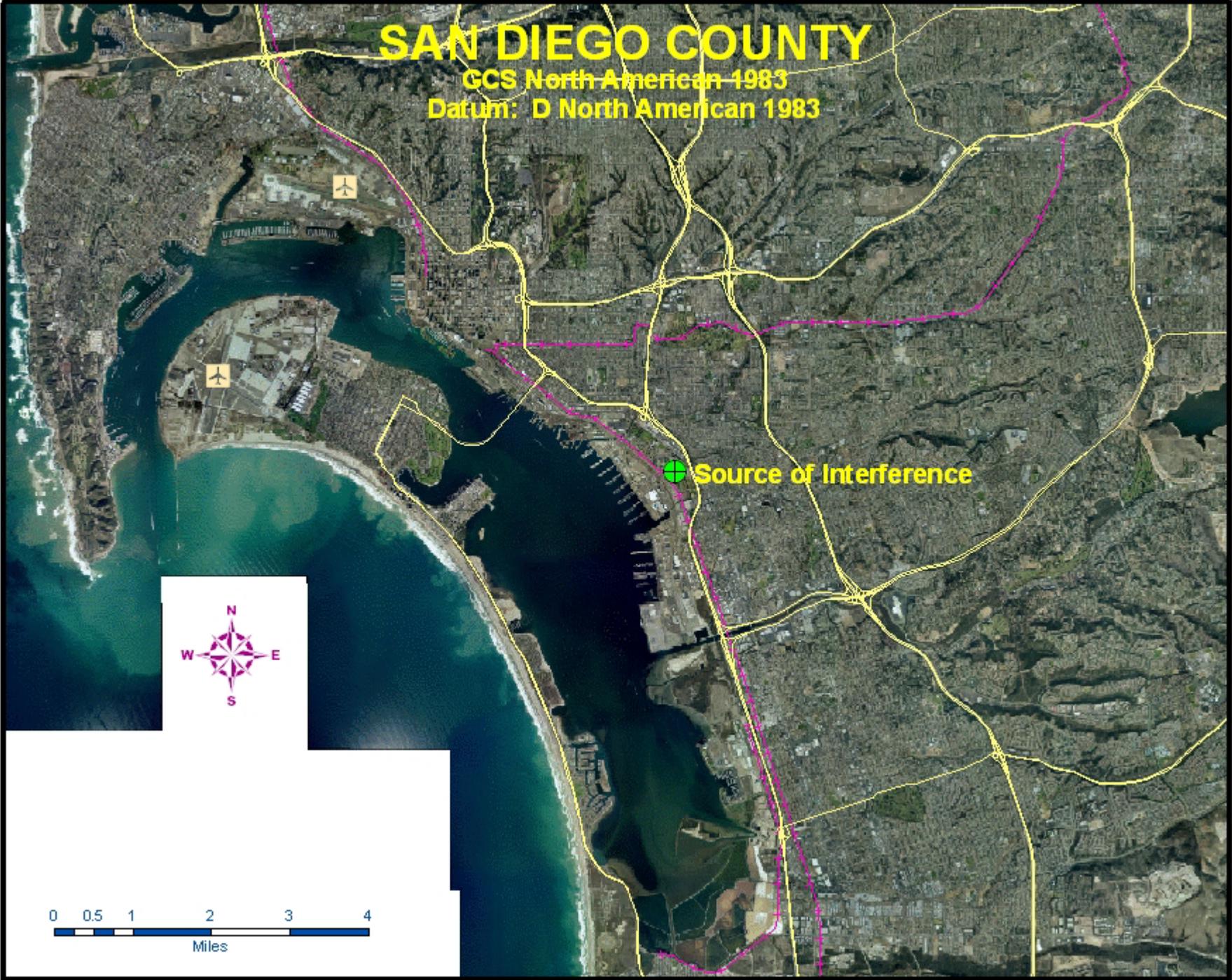
Legend

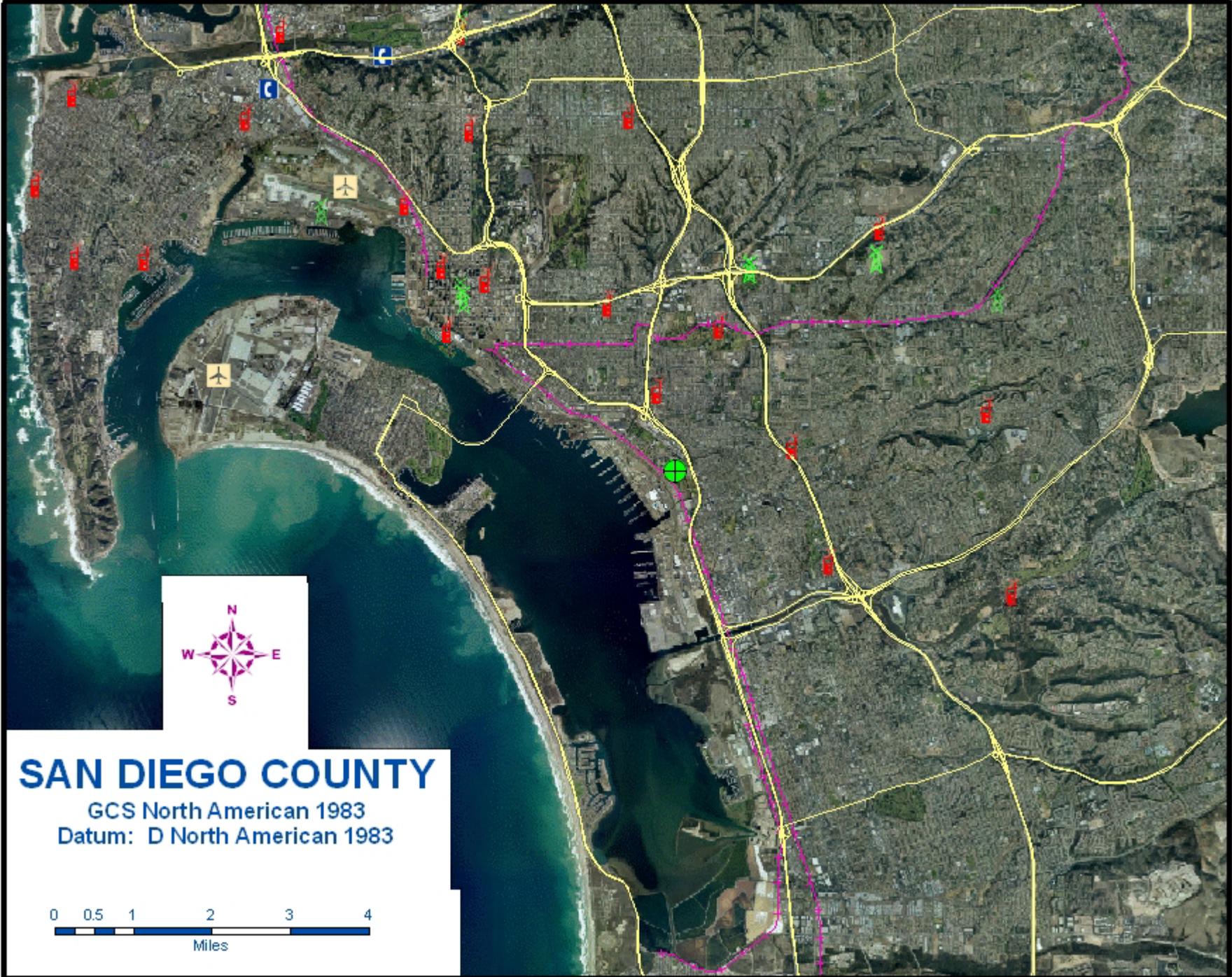


SAN DIEGO COUNTY

GCS North American 1983
Datum: D North American 1983

Source of Interference

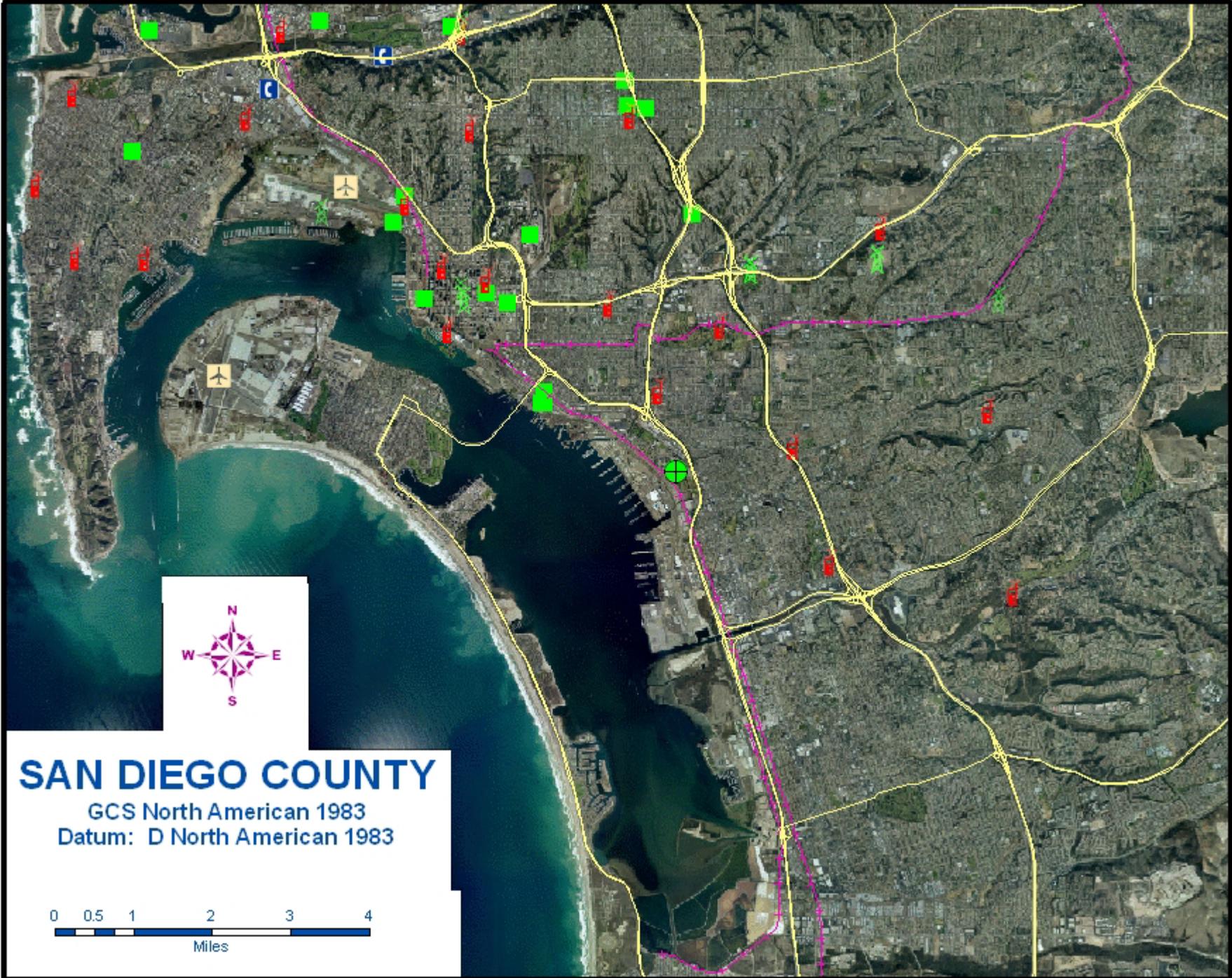




SAN DIEGO COUNTY

GCS North American 1983
Datum: D North American 1983

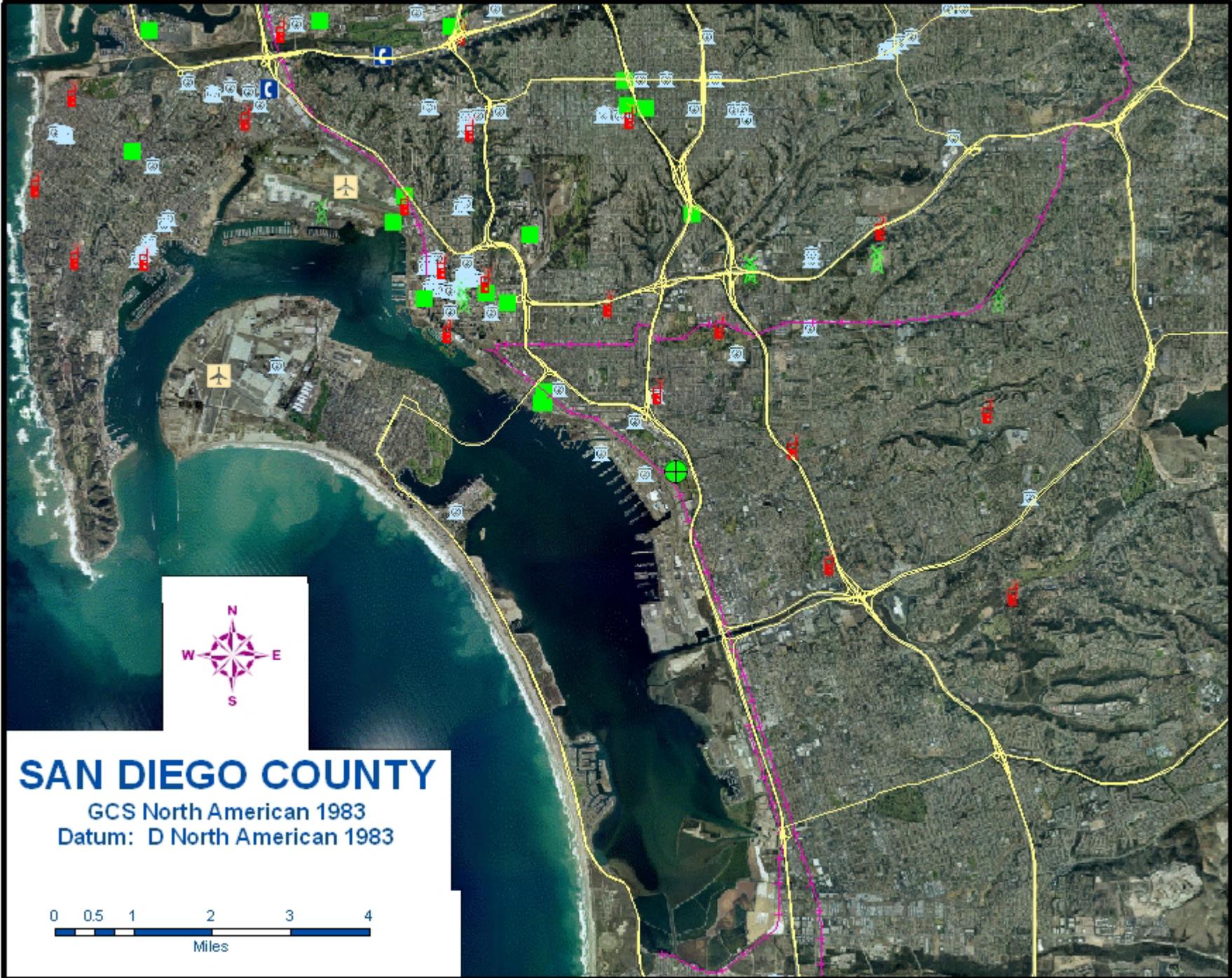




SAN DIEGO COUNTY

GCS North American 1983
Datum: D North American 1983

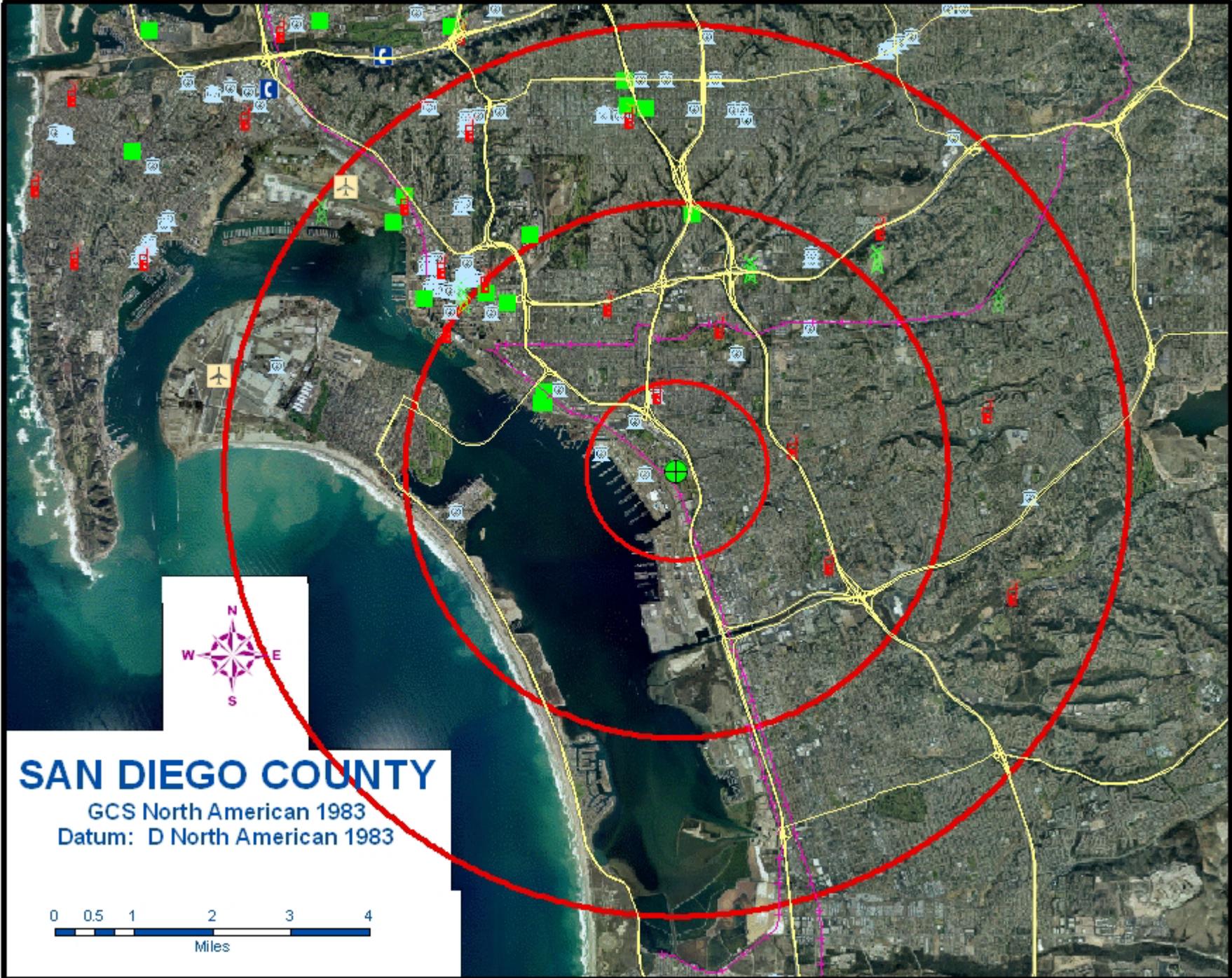




SAN DIEGO COUNTY

GCS North American 1983
Datum: D North American 1983





SAN DIEGO COUNTY

GCS North American 1983
Datum: D North American 1983



Patriot Watch System

- **System-of-Systems approach to provide real-time monitoring (preparedness), location & notification (response) of GPS interference for protecting the Nations CIKR Sectors.**
 - Designed with government & commercial hardware
 - Persistent monitoring yields situational awareness
 - Timely response to anomalies
 - Sensor placement based on PNT CIKR Criticality
 - Remains operational when GPS systems is “stressed”
- **Collective Effort by various USG entities**
- **Significant Cost and Risk reduction by taking full advantage of mature, existing systems**

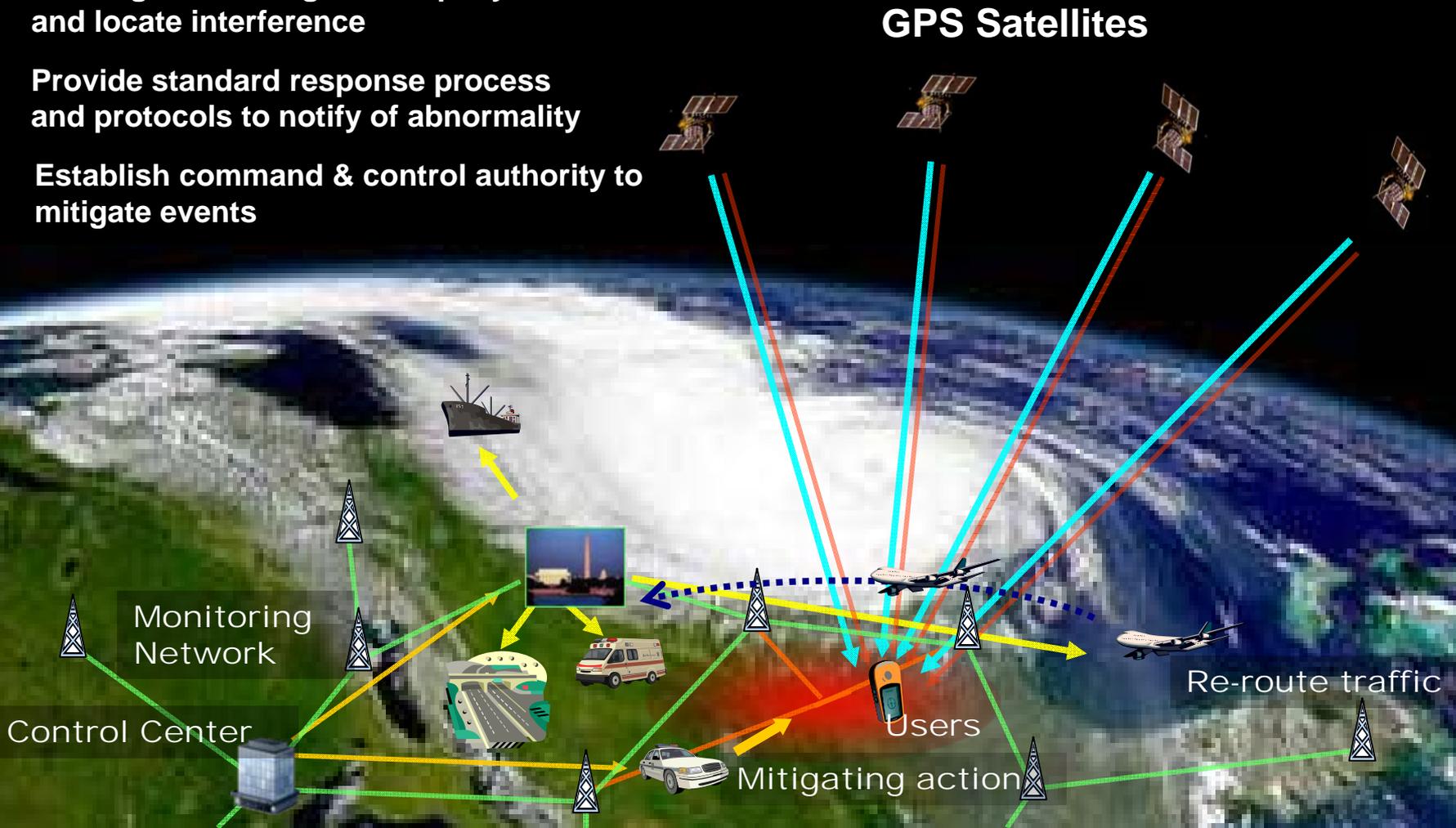
Patriot Watch - Concept

National capability to detect & mitigate GPS interference INCONUS, supporting PNT and CIKR resilience

Leverage technologies to rapidly detect and locate interference

Provide standard response process and protocols to notify of abnormality

Establish command & control authority to mitigate events



QUESTIONS?

Rick.Hamilton@uscg.mil

703-313-5930

John.Merrill@dhs.gov

202-447-3731

