Department of Homeland Security (DHS) GPS Interference Detection and Mitigation (IDM) Program

Chief Brian Penick
GPS Information Analysis Team
U.S. Coast Guard Navigation Center

John Merrill
DHS PNT Program Manager
Office of Applied Technology Geospatial Management Office

Homeland Security

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

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?

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 not-quite-technical term first coined in the radar community, is the transmission of fake GPS signals that receivers accept as authentic ones.

Todd Humphreys, right, discusses with Paul Kintner, left, and Mark Psiaki how a GPS receiver can be "spoofed," based on the research work of Cornell Robert Barker/University Photography

The Washington

Gunmen Used Technology as A Tactical Tool

Haste Could Make Waste

Obama Teams Are Scrutinizing

Coaxing!

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

WA Post Aug 08

Police Turn to Secret Weapon: GPS Device

By Ellen Nakashima
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 Foltz Jr., who had served 17 years in prison for rape, lived near the crime scenes. To figure out if Foltz was the assailant, police pulled out their secret weapon: They put a Global Positioning System device on Foltz's van, which allowed them to track his movements.

Police said they soon caught Foltz 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.

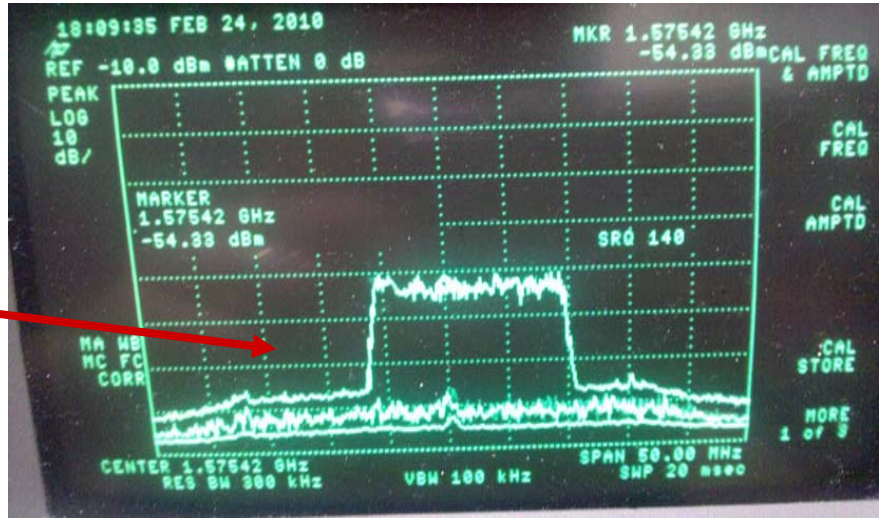
"We don't really want to give any info on how we use it as an investigative tool to help the bad guys," said Officer Shelley Buckallew, a Fairfax police spokeswoman. "It is an investigative booster as, and it is a very new investigative tool."

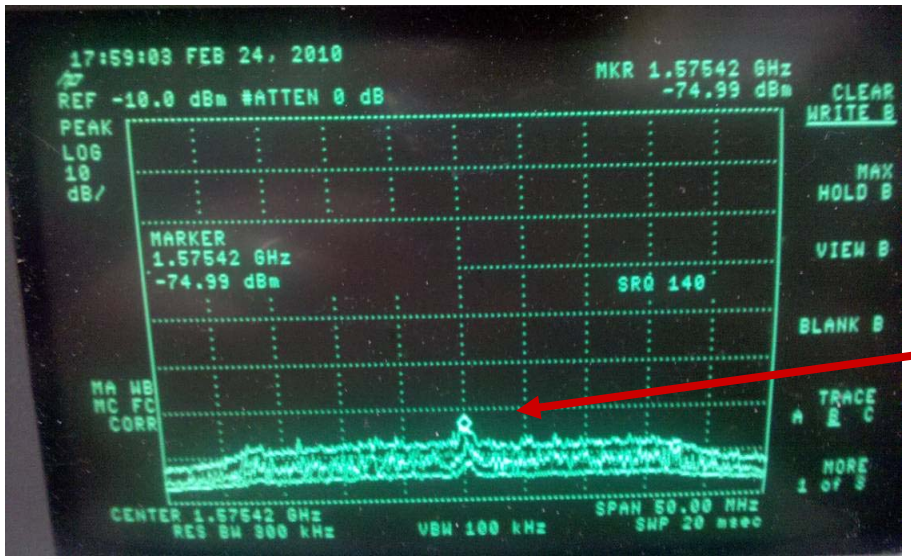
Across the country, police are using GPS devices to snare thieves, drug dealers, sexual predators and killers, often without a warrant or court order. Privacy advocates said tracking suspects electronically ...

See GPS DEVICES, A12, Col. 1

US Government Measurements

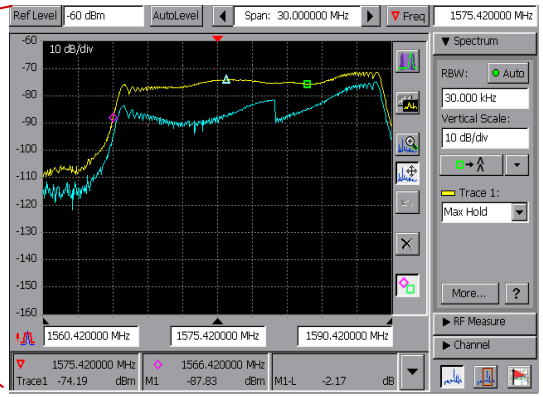
Wideband RFI Source measured occupying approximately 20 MHz – 5 MHz below L1 and 15 MHz above L1.



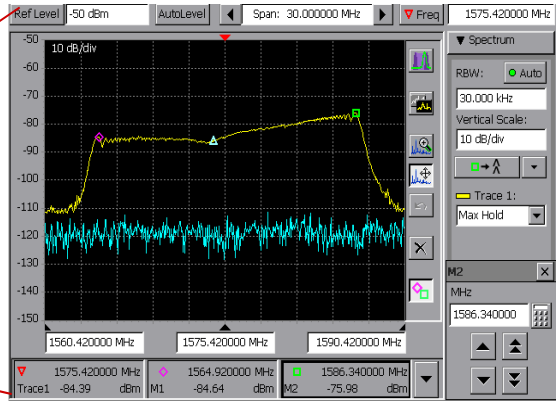


Normal L1 passband Spectrum when RFI Source is not present.

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

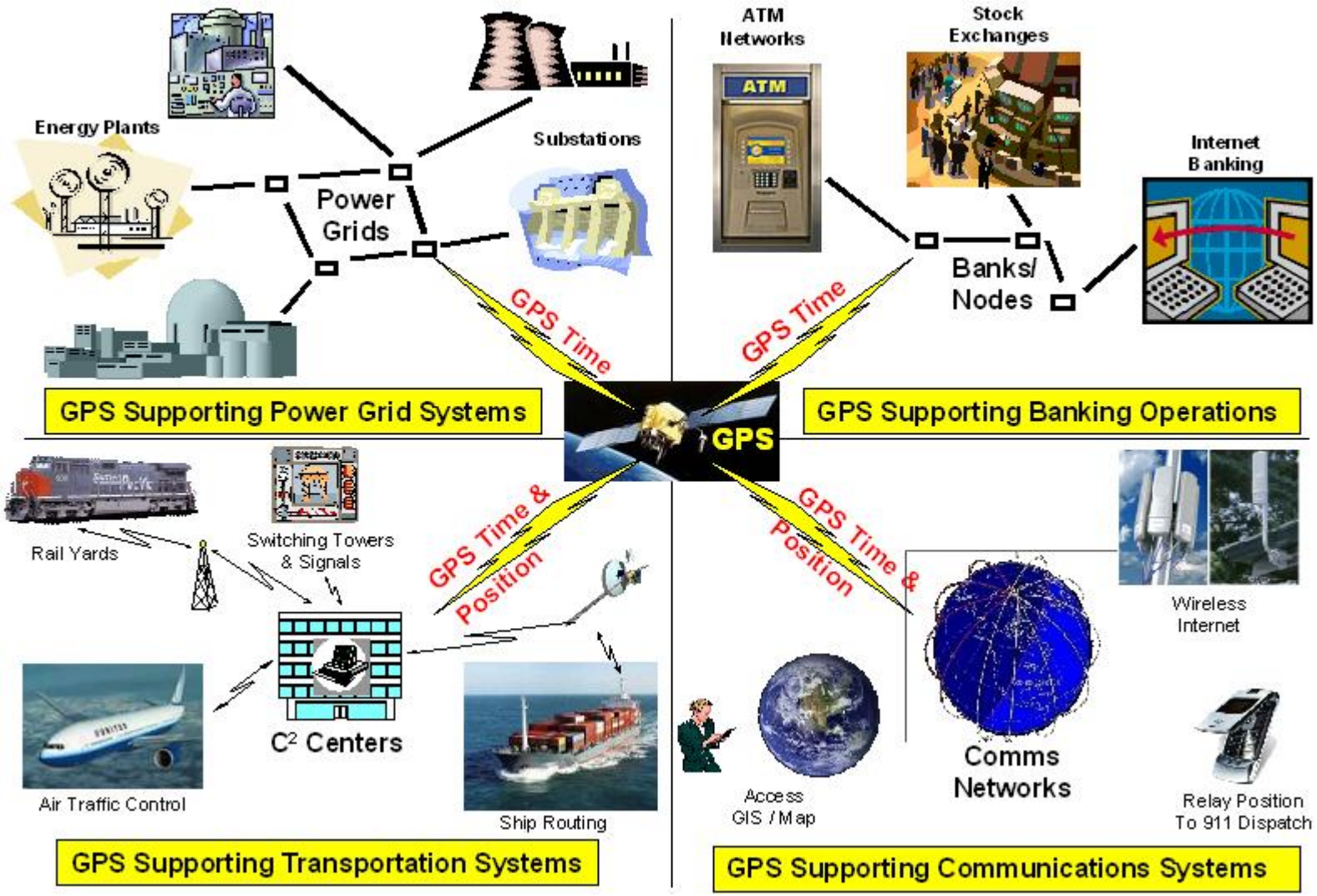

Nuclear Reactors, Materials and Waste


Postal and Shipping


Transportation Systems


Water

Extent of GPS Dependencies



The GPS Triad

Joint GPS User Support Service

USAF GPSOC
(military)

FCC

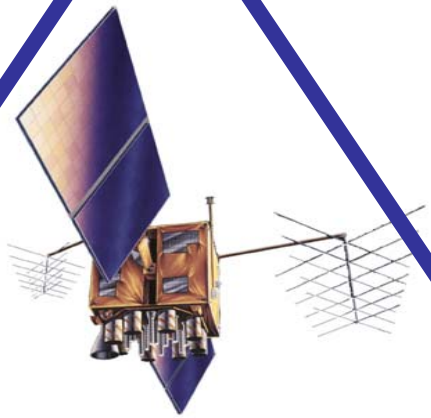
PIRT

NTIA

NORAD/NORTHCOM

USSTRATCOM

JSC



USCG NAVCEN
(surface)

FAA NOCC
(airspace)

Patriot Watch Customer Base/Users

GPS Civil Performance

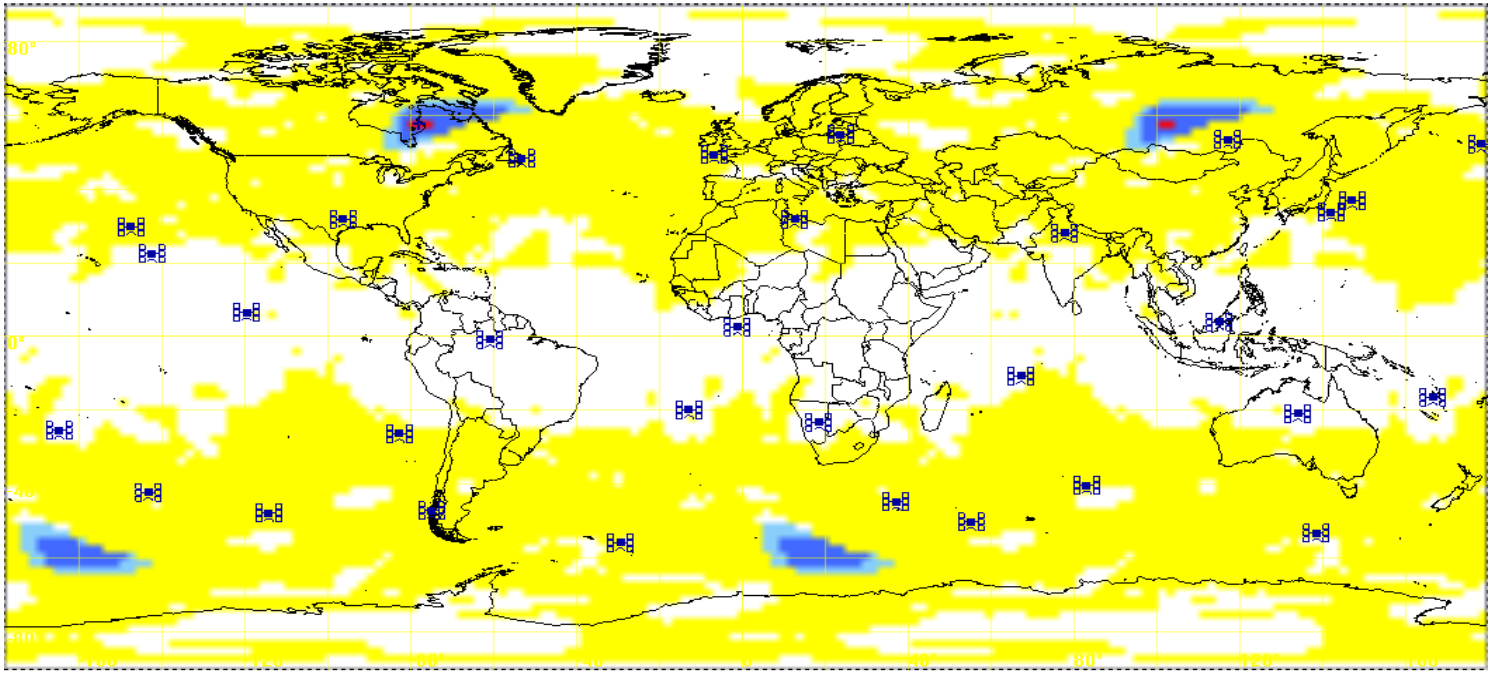
- The TRIAD uses DOD developed tools to predict GPS performance impacts due to satellite constellation status
- Enables prediction of Horizontal Dilution of Precision (HDOP); measure of surface user accuracy.
- HDOP out of tolerance (more than 6) triggers a coordinated regional user notification (Notice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

NAVCEN DAILY SYSTEMS BRIEF

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			

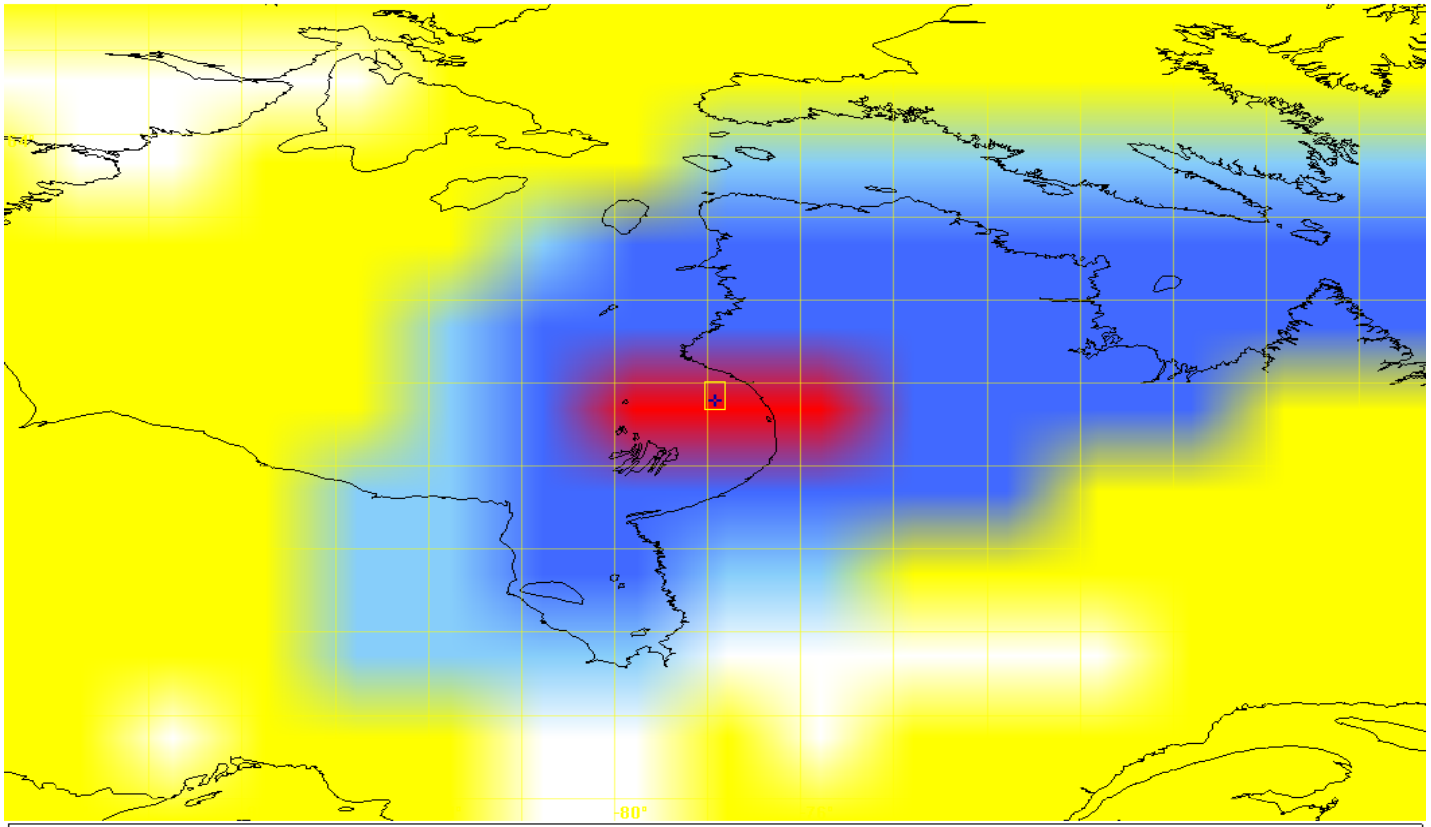
UNCLASSIFIED UNCLASSIFIED

NAVCEN DAILY SYSTEMS BRIEF

GPS HDOP

Prediction

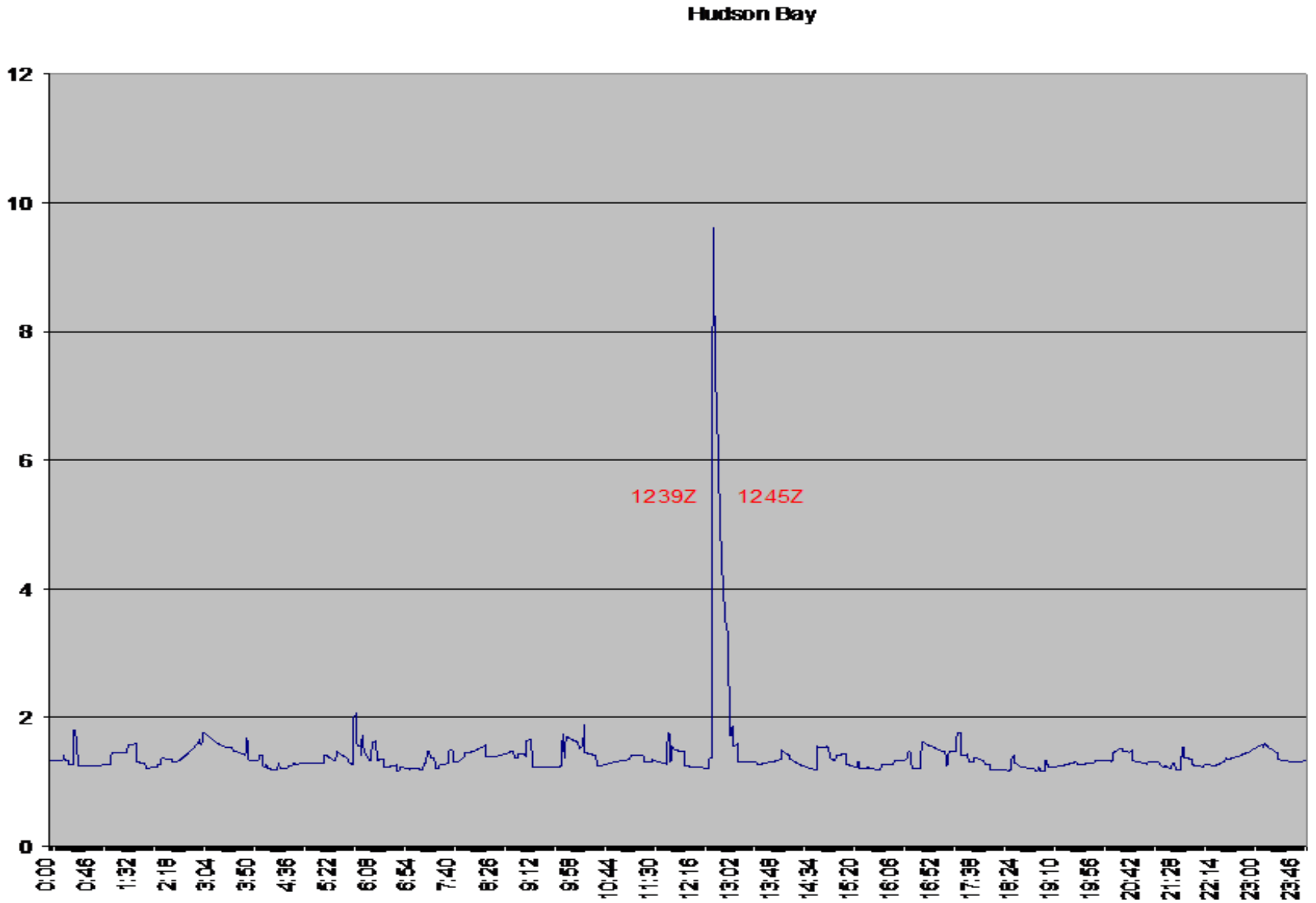
16 AUG 2010



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


Hudson Bay
12
10
8
6
4
2
0
1239Z
1245Z
0:00
0:46
1:32
2:18
3:04
3:50
4:36
5:22
6:08
6:54
7:40
8:26
9:12
9:58
10:44
11:30
12:16
13:02
13:48
14:34
15:20
16:06
16:52
17:38
18:24
19:10
19:56
20:42
21:28
22:14
23:00
23:46

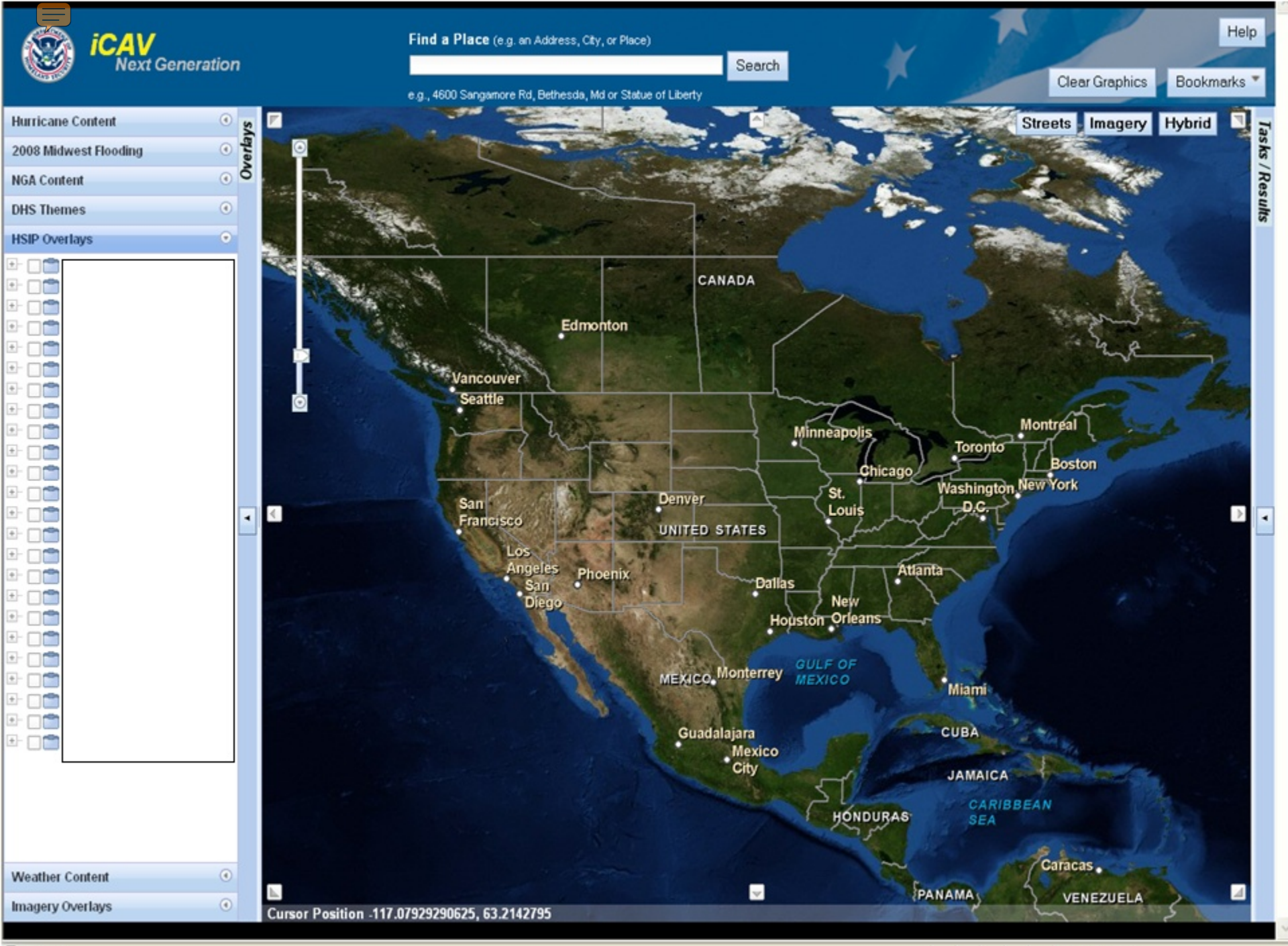
Central Data Repository Requirements
(Policy Derived Qualitative)

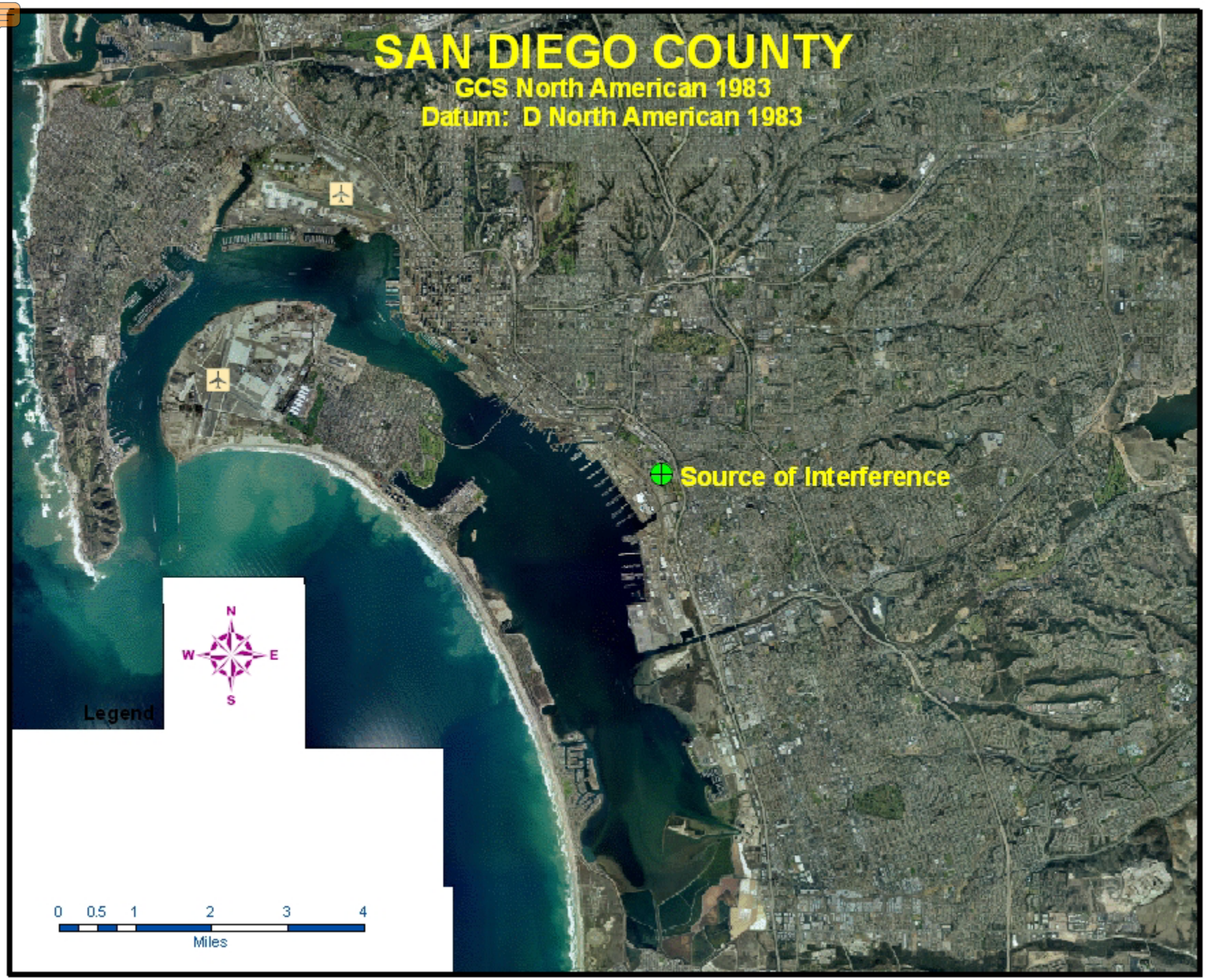
- Central Interference Reporting database for all PNT incidents
- Encompass process and functions for detection validation, investigation, assessment, corroboration of PNT incidents
- Automated dissemination of data and reduce PNT incidents information distribution delays for decision support
- Mechanisms 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

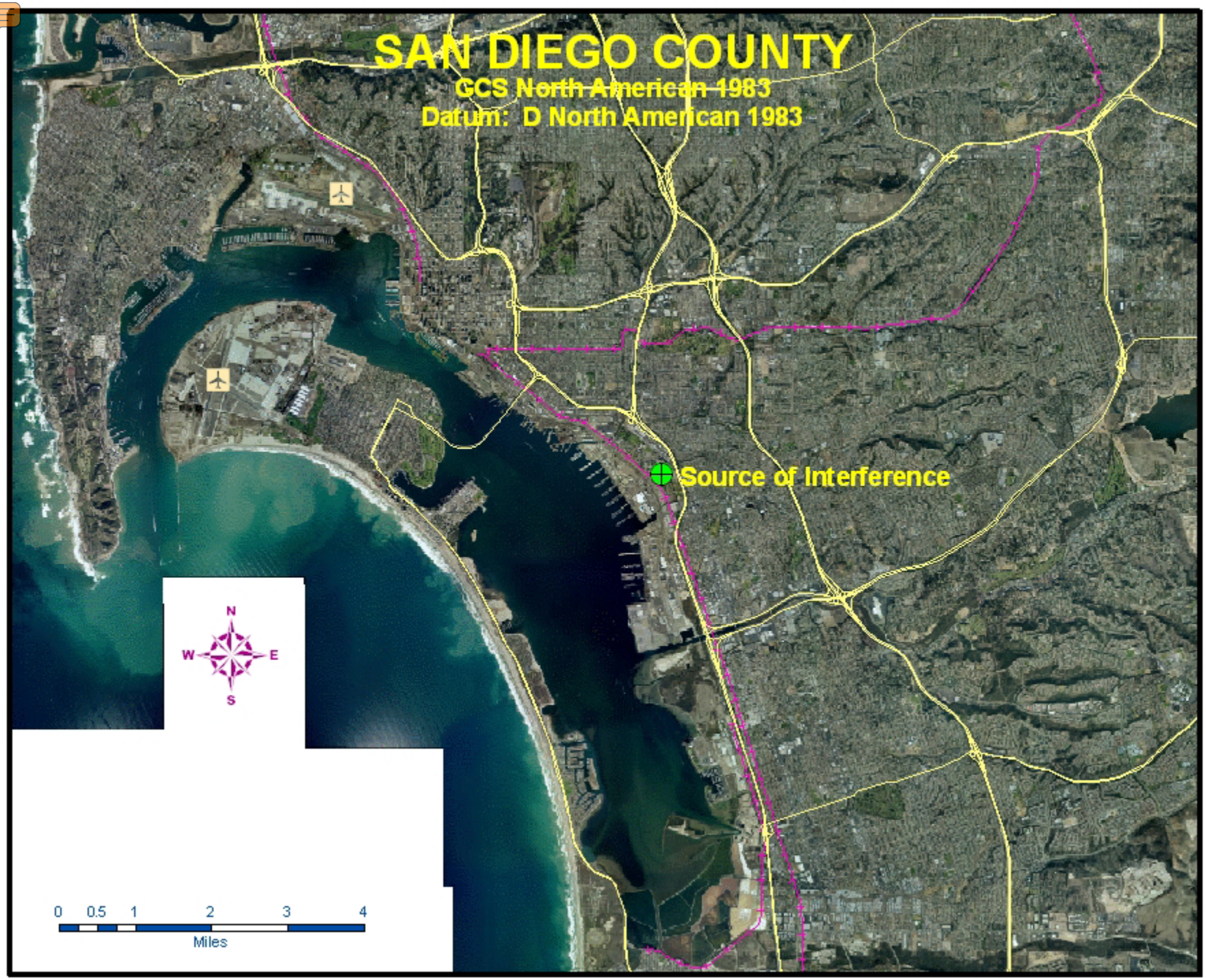
Secure User Authentication

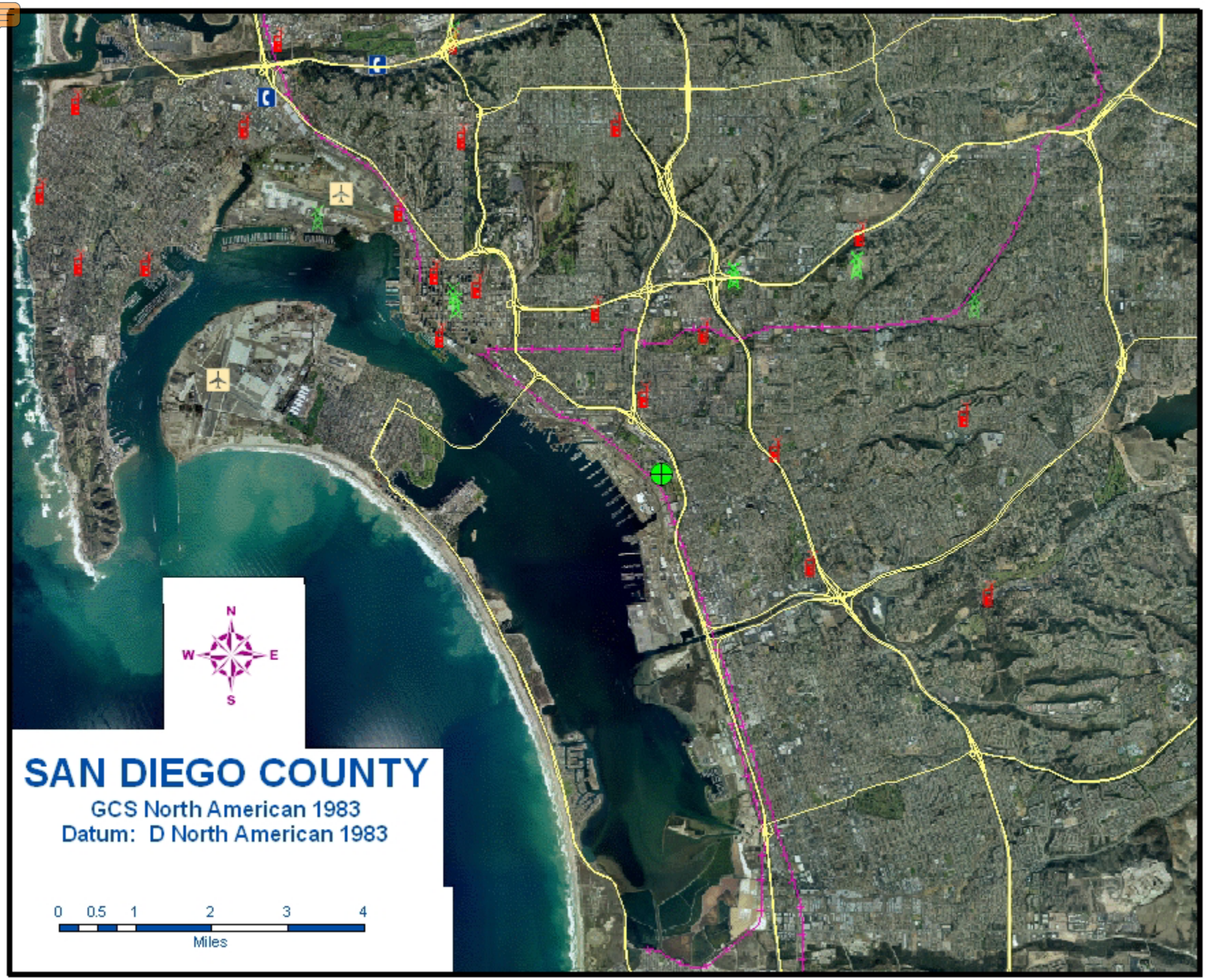
Central Data Repository

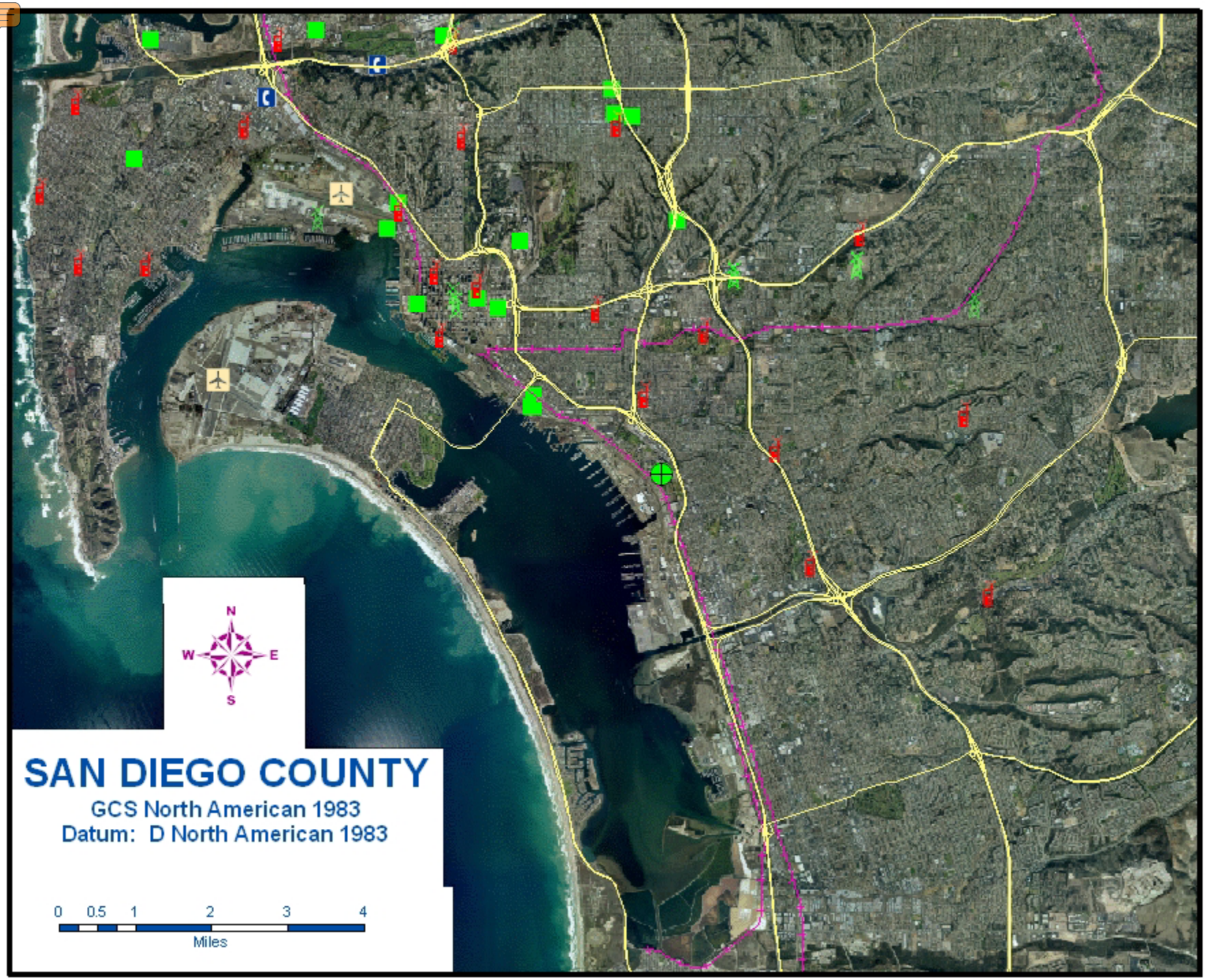
- Baseline Requirements – Cost control, use existing architecture
- Designed Leverage – Modeled based on the FAA Spectrum Engineering Tracking System (SETS)
- Visual Operational Picture – Integrated Common Analytical Viewer (iCAV)
  - Geospatial enabling/visualization tool
  - Integrates multiple geospatial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

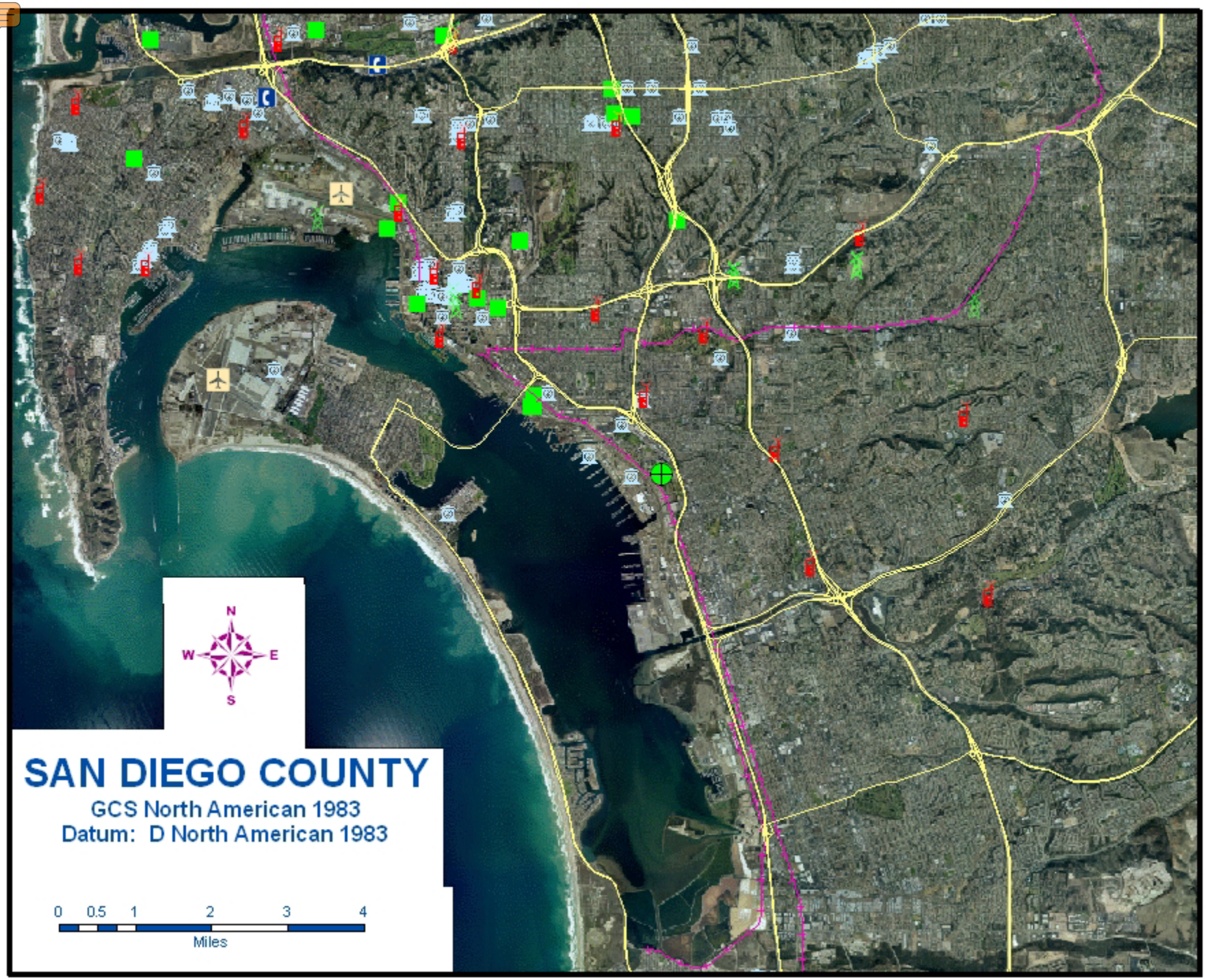

iCAV
Next Generation
Find a Place (e.g. an Address, City, or Place)
Search
e.g., 4600 Sangamore Rd, Bethesda, Md or Statue of Liberty
Help
Clear Graphics
Bookmarks
Hurricane Content
2008 Midwest Flooding
NGA Content
DHS Themes
HSIP Overlays
Overlays
Weather Content
Imagery Overlays
Streets
Imagery
Hybrid
Tasks / Results
CANADA
Edmonton
Vancouver
Seattle
Minneapolis
Montreal
Toronto
Chicago
Boston
New York
Washington D.C.
St. Louis
Denver
San Francisco
UNITED STATES
Los Angeles
San Diego
Phoenix
Dallas
Atlanta
New Orleans
Houston
GULF OF MEXICO
MEXICO
Monterrey
Miami
Guadalajara
Mexico City
CUBA
JAMAICA
CARIBBEAN SEA
HONDURAS
Caracas
PANAMA
VENEZUELA
Cursor Position -117.07929290625, 63.2142795
Done
Internet

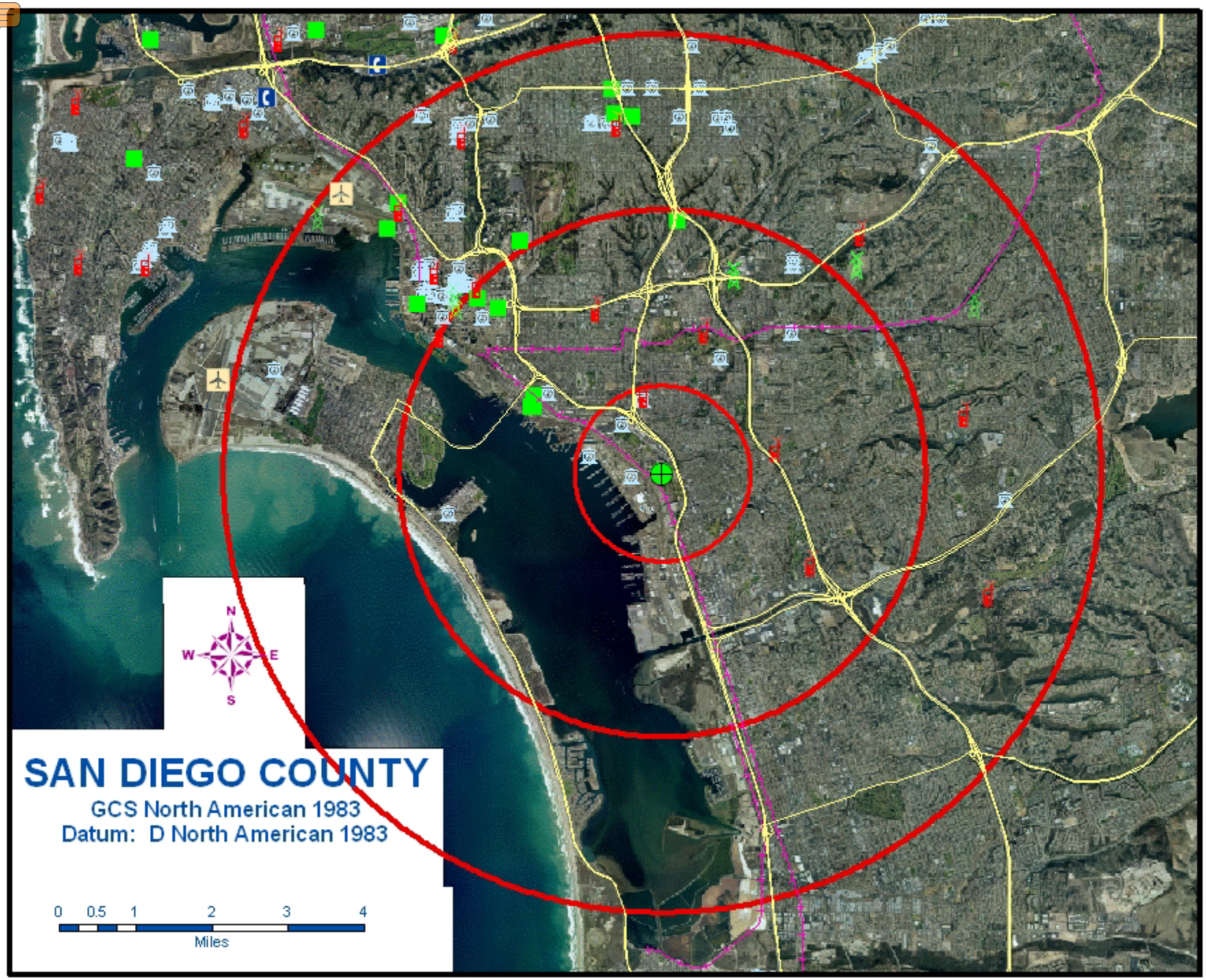

SAN DIEGO COUNTY
GCS North American 1983
Datum: D North American 1983
Source of Interference
N
W
E
S
Legend
0 0.5 1 2 3 4
Miles


SAN DIEGO COUNTY
GCS North American 1983
Datum: D North American 1983
Source of Interference
N
W
E
S
0 0.5 1 2 3 4
Miles


N
W
E
S
SAN DIEGO COUNTY
GCS North American 1983
Datum: D North American 1983
0 0.5 1 2 3 4
Miles


N
W
E
S
SAN DIEGO COUNTY
GCS North American 1983
Datum: D North American 1983
0 0.5 1 2 3 4
Miles


N
W
E
S
SAN DIEGO COUNTY
GCS North American 1983
Datum: D North American 1983
0 0.5 1 2 3 4
Miles


N
W
E
S
SAN DIEGO COUNTY
GCS North American 1983
Datum: D North American 1983
0 0.5 1 2 3 4
Miles

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

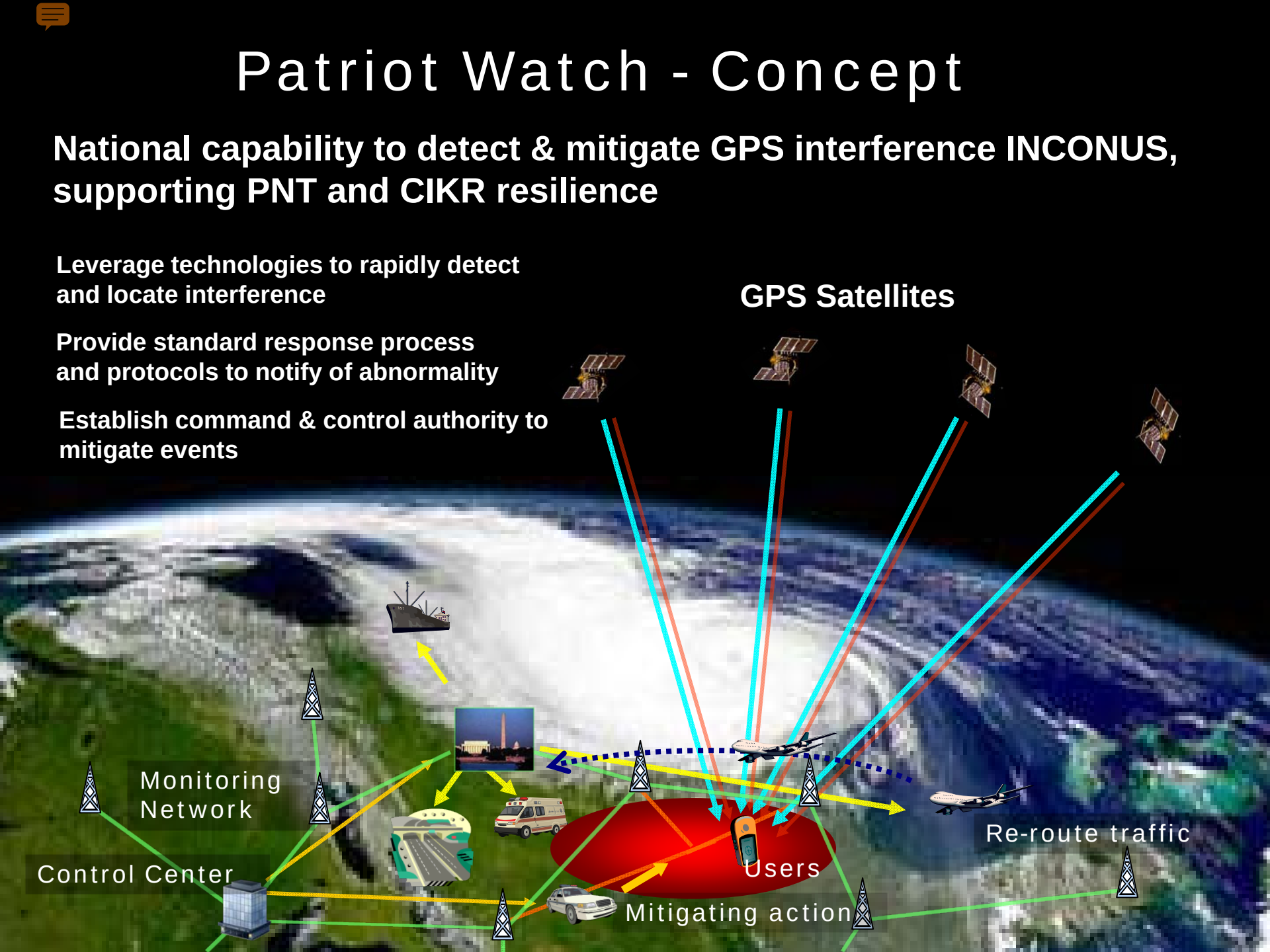
Patriot Watch - Concept

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?

brian.penick@schriever.af.mil

703-313-5930

John.Merrill@dhs.gov

202-447-3731