DEPARTMENT OF HOMELAND SECURITY

INTERFERENCE DETECTION & MITIGATION (IDM)

IN COLLABORATION WITH OTHER FEDERAL AGENCIES

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

CGSIC September 2013

Homeland Security

Agenda

- DHS Office of Safety Act Implementation (OSAI)
- Federal Communications Commission Enforcement Bureau (FCC EB)
- Geospatial Information Infrastructure (GII)
  - Patriot Watch
    - Radio Frequency Interference Tracking (RFIT), formerly the PNT Incident Portal (PNT IP)
    - COTS Jammer Digital Library
    - Unclassified Jammer Location (JLOC)
    - HammerHead tactical unit for jammer location
- Collaboration equals success

DHS Office of SAFETY Act Implementation (OSAI)

- **To support Anti-terrorism by fostering Effective Technologies Act of 2002 established the SAFETY Act Program. Companies involved in the development of anti-terrorism products or services and other forms of intellectual property *may qualify* for SAFETY Act liability protection.**
- **OSAI's primary goal is to ensure the widespread deployment of effective anti-terrorism technologies and services by offering two levels of liability protection to help promote the creation, deployment and use of anti-terrorism technologies. These levels are call Designation and Certification**
- **These products, services and software technologies must be determined to be Qualified Anti-Terrorism Technologies (QATT) through an evaluation process conducted by DHS using subject matter experts.**
- **SAFETY Act coverage supports both government and private investments in critical research and development programs, recognized national labs, and research and development projects undertaken by the private sector.**

Homeland Security

OSAI POC: Thomas Chirhart, *Emerging Technologies Program Manager*
DHS Science and Technology Directorate; 202-254-6063 *www.safetyact.gov*

What is Eligible for Safety Act Protections

The SAFETY Act liability protections apply to a wide range of technologies, including:

- Products
- Services
- Software and other forms of intellectual property

Examples of eligible technologies:

Threat and Vulnerability Assessment Services

Detection Systems

Blast Mitigation Materials

Screening Services

Sensors and Sensor Integration

Threatening Object Detectors

Decision Support Software

Security Plans / Services

Crisis Management Systems

Venue Security

Homeland Security

OSAI POC: Thomas Chirhart, *Emerging Technologies Program Manager*
DHS Science and Technology Directorate; 202-254-6063 *www.safetyact.gov*

Education and Outreach Efforts

Coupled with increasingly aggressive enforcement action, the FCC Enforcement Bureau (EB) continues to educate the public, coordinate with other USG agencies, and form international partnerships. For example, EB has:

- **released three Enforcement Advisories (one of which was translated into Spanish and Mandarin) designed to (i) educate retailers and consumers, (ii) emphasize that jammers are illegal, and (iii) note that violators risk substantial civil and criminal penalties;**
- **launched a webpage focused on jammer enforcement (http://www.fcc.gov/jammers);**
- **developed and released detailed Frequently Asked Questions on signal jamming devices;**
- **created jammerinfo@fcc.gov, a one-stop shop for consumer questions regarding jammers;**
- **instituted a dedicated tip line for jammers: 1-855-55NOJAM (1-855-556-6526);**
- **issued a downloadable poster highlighting the jamming prohibition and describing how to file a complaint; and**
- **developed jammer-related reference bulletins for law enforcement officers and other critical audiences.**

ENFORCEMENT BUREAU
SIGNAL JAMMER ENFORCEMENT INITIATIVE

Spotting a Signal Jamming Device

Possible—but not definitive—indications of jammer activity. (Problems unrelated to jammers may also cause these conditions.)

- **inability to transmit or receive on two-way radios outside of known "dead zones";**
- **unusual sounds on designated frequencies, such as unintelligible electronic white noise, intermittent electronic chirping, or unusual tones;**
- **technical difficulties that appear and disappear intermittently;**
- **lack of audible click when keying a microphone;**
- **abrupt loss of communications, especially if stationary; and**
- **loss of lock, intermittent disruption, or general failure of a GPS receiver or GPS-enabled device.**

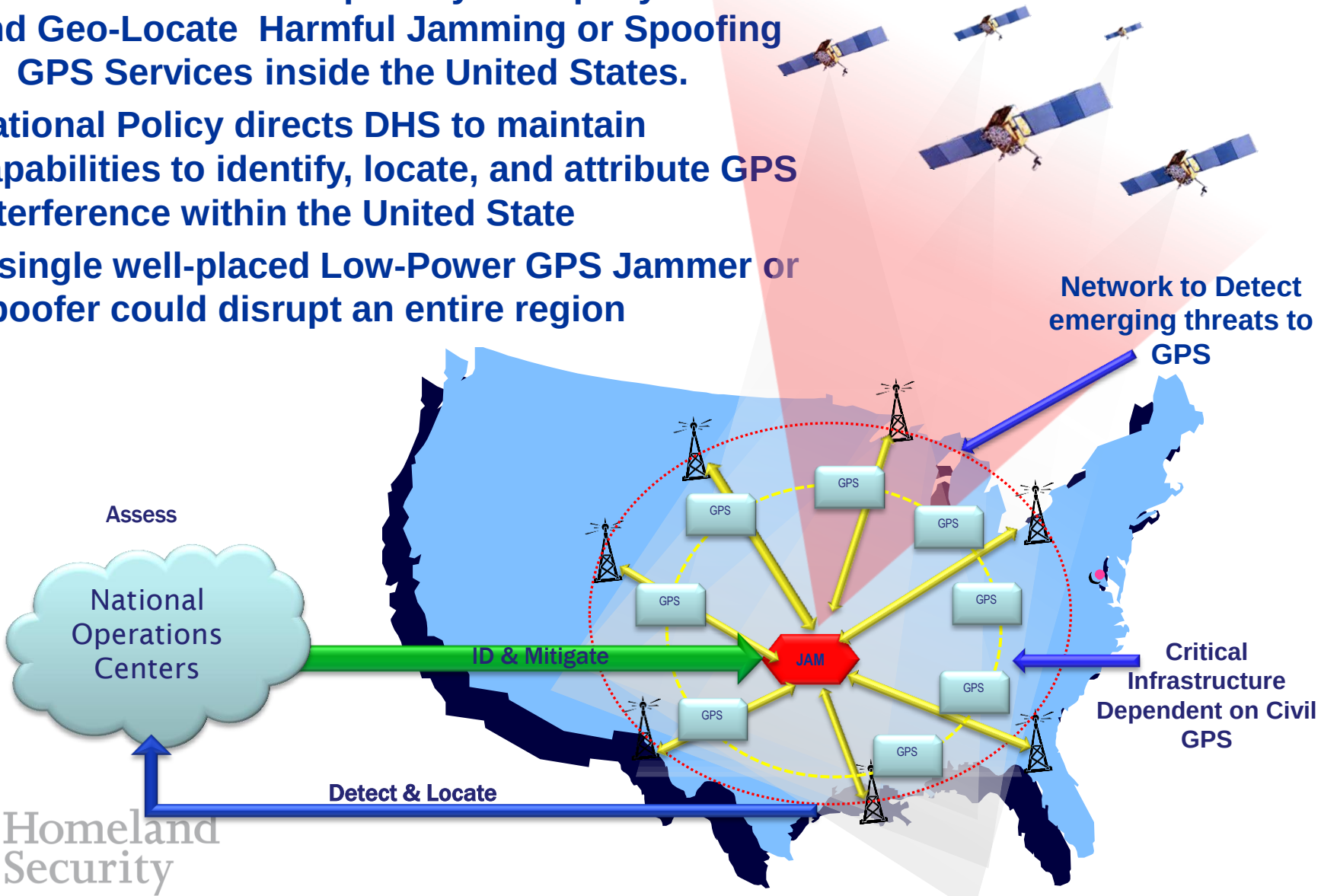
Images of Common RF Jamming Devices

To report the use or marketing of any signal jammer, call the FCC Jammer Tip Line: 1-855-55-NOJAM (1-855-556-6526)

Homeland Security

Patriot Watch Overview

- **The U.S. Lacks the Capability to Rapidly Detect and Geo-Locate Harmful Jamming or Spoofing of GPS Services inside the United States.**
- **National Policy directs DHS to maintain capabilities to identify, locate, and attribute GPS interference within the United State**
- **A single well-placed Low-Power GPS Jammer or Spoofer could disrupt an entire region**



Homeland Security

Geospatial Information Infrastructure (GII)

Key Benefits:

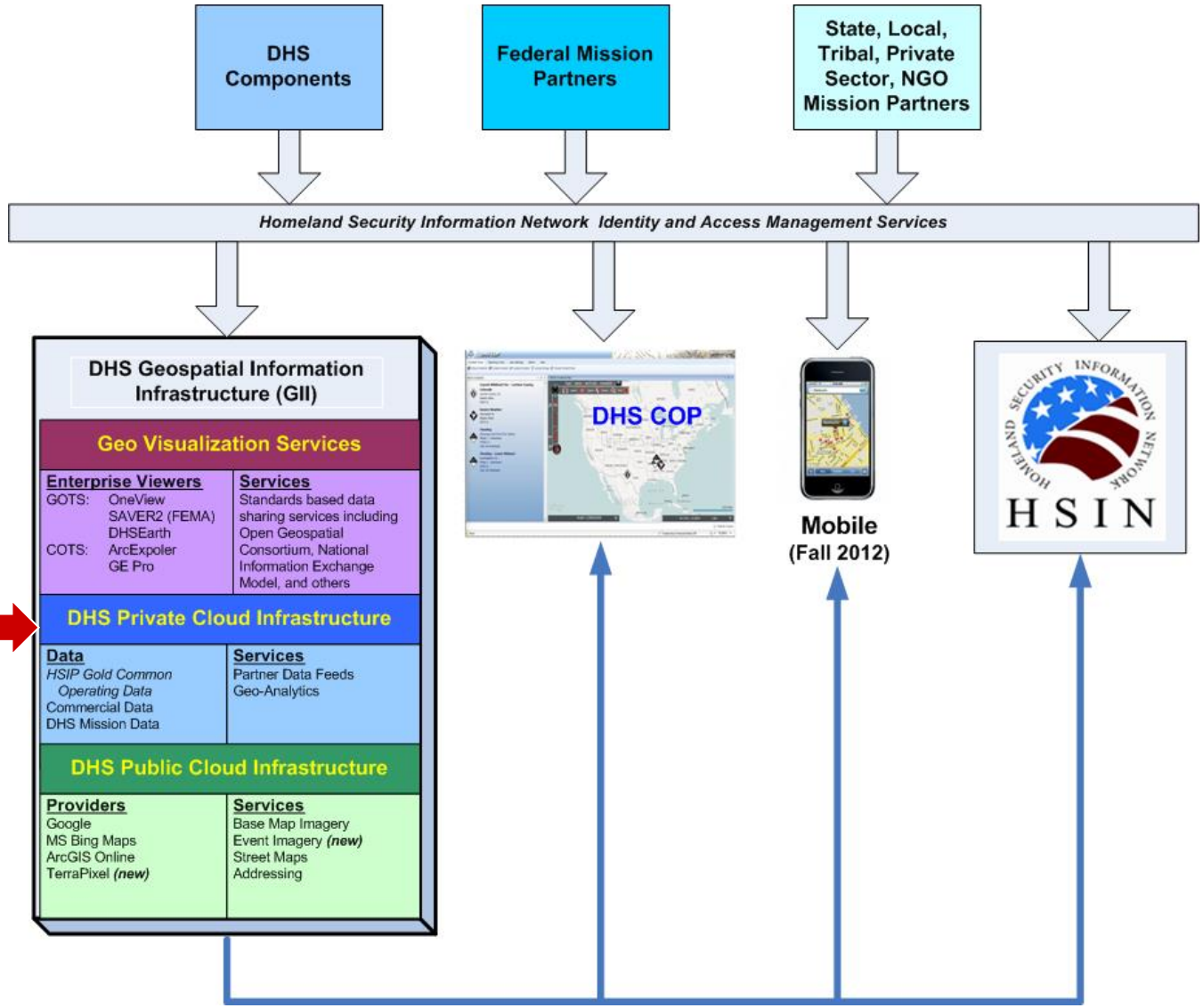
The GII is physically located in the DHS Data Centers

Accessible through the HSIN identity service

Provides viewing tools, data and analytical services

Supports the DHS COP and HSIN

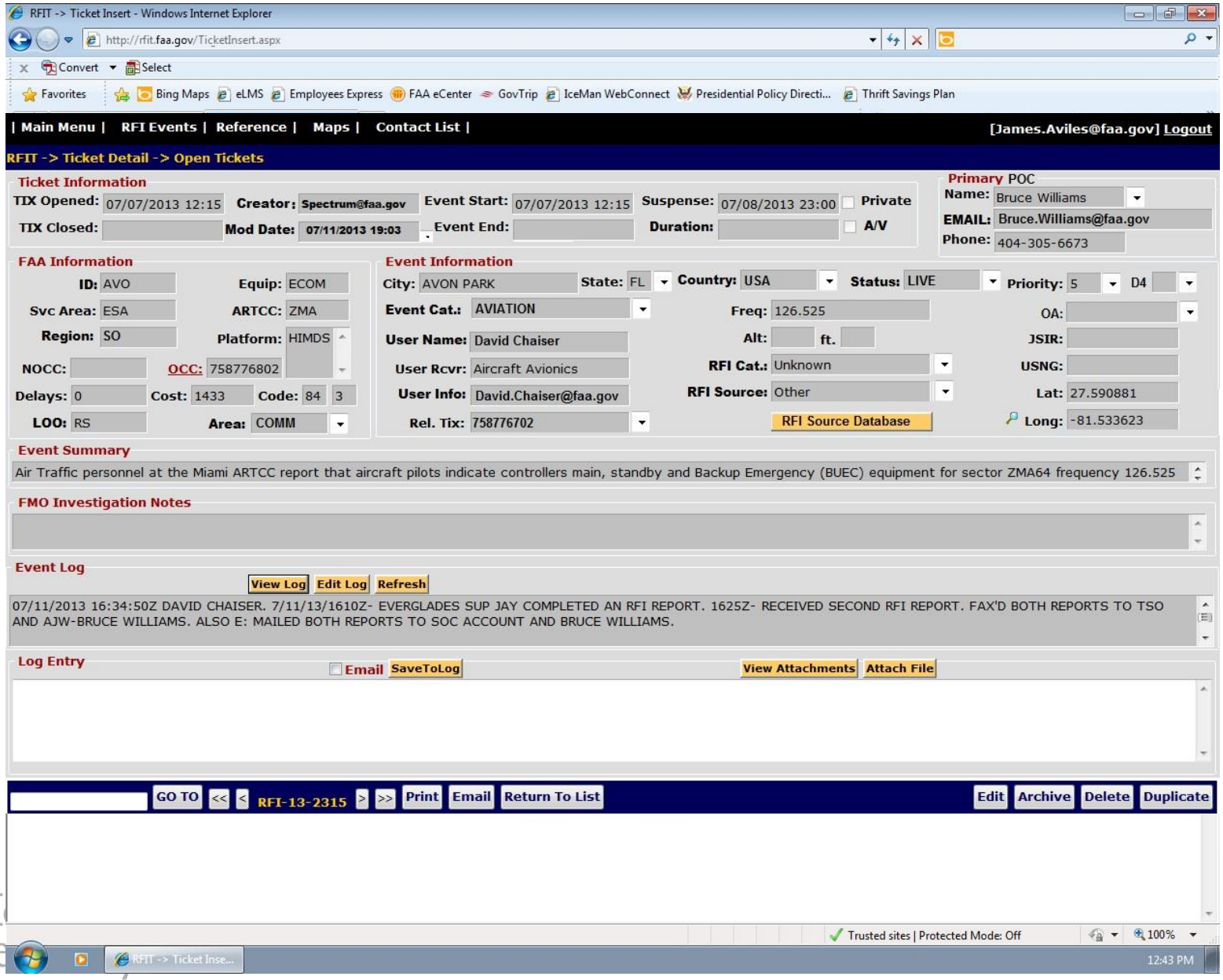
Supports User Defined Operating Pictures (UDOP) across the Homeland Security Enterprise



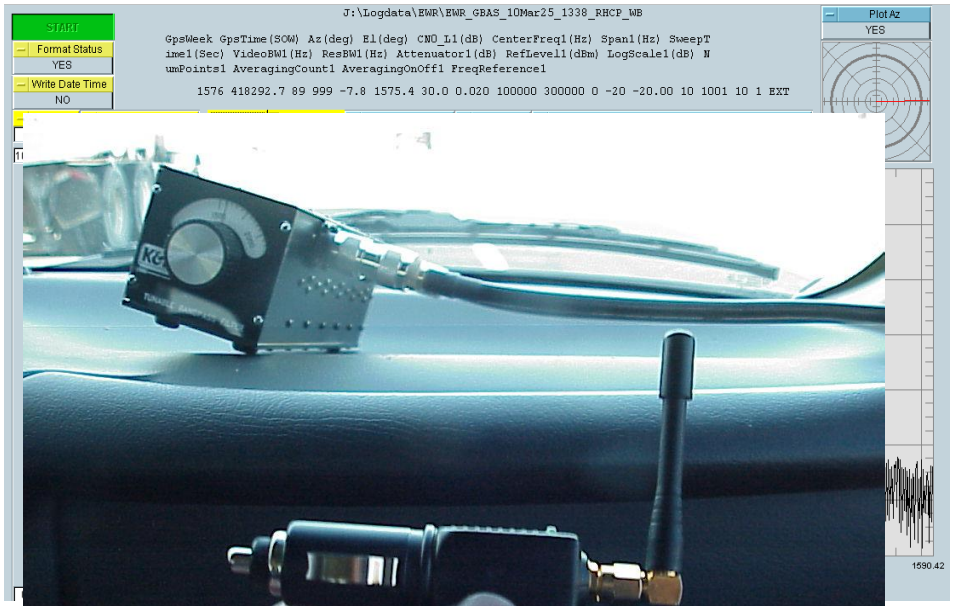
Homeland Security

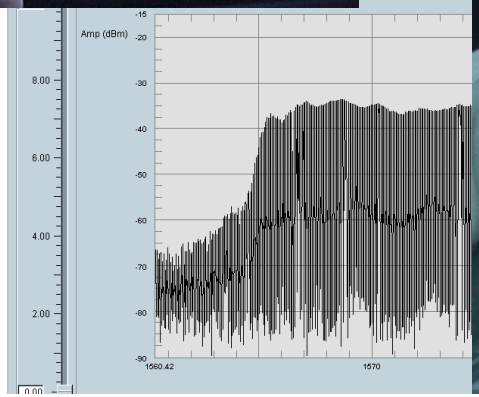
Radio Frequency Tracking System (RFIT)

Source: FAA Spectrum Engineering Office



GPS COTS Jammer Digital Library



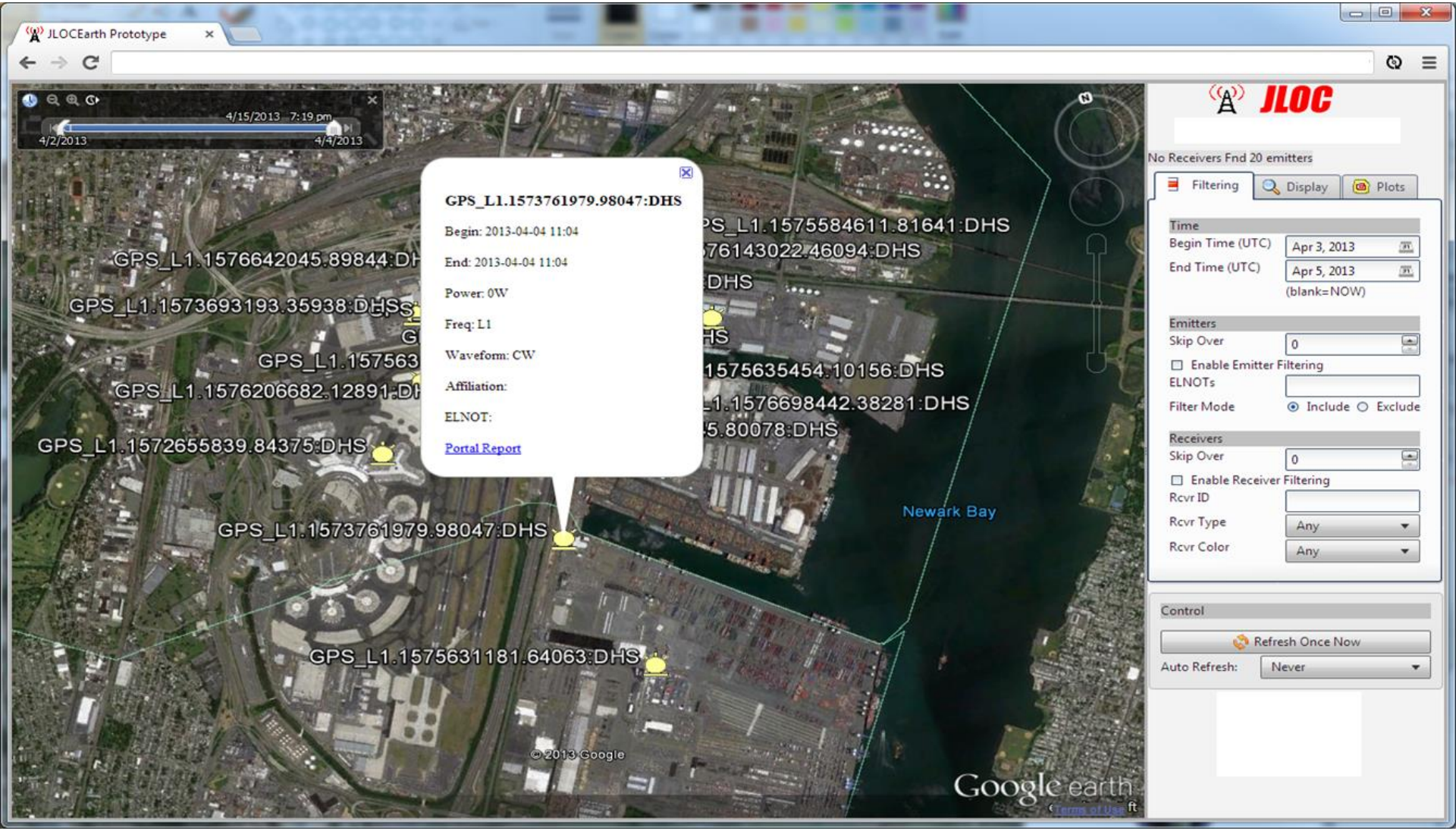


Homeland Security

Jammer Location (JLOC)

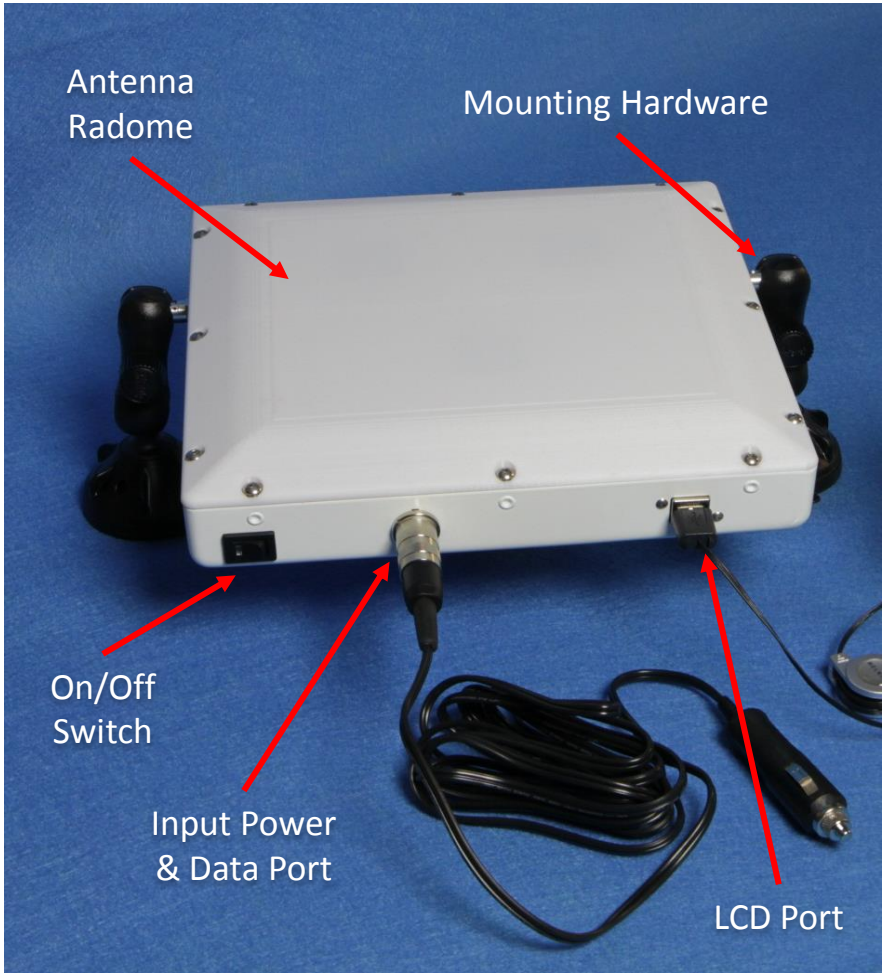
- The GPS JLOC System has been in development since 2010
- Joint project between DHS and DoD to create an unclassified version of the program to be used for collecting CONUS GPS interference data
- Utilize sensor feeds from DHS's Patriot Watch program
  - Prototype data is coming from sensors at the Newark, NJ airport (EWR)
  - Sensor data feeds DHS UniTrac system
  - UniTrac feeds JLOC or any other Geospatial Information System

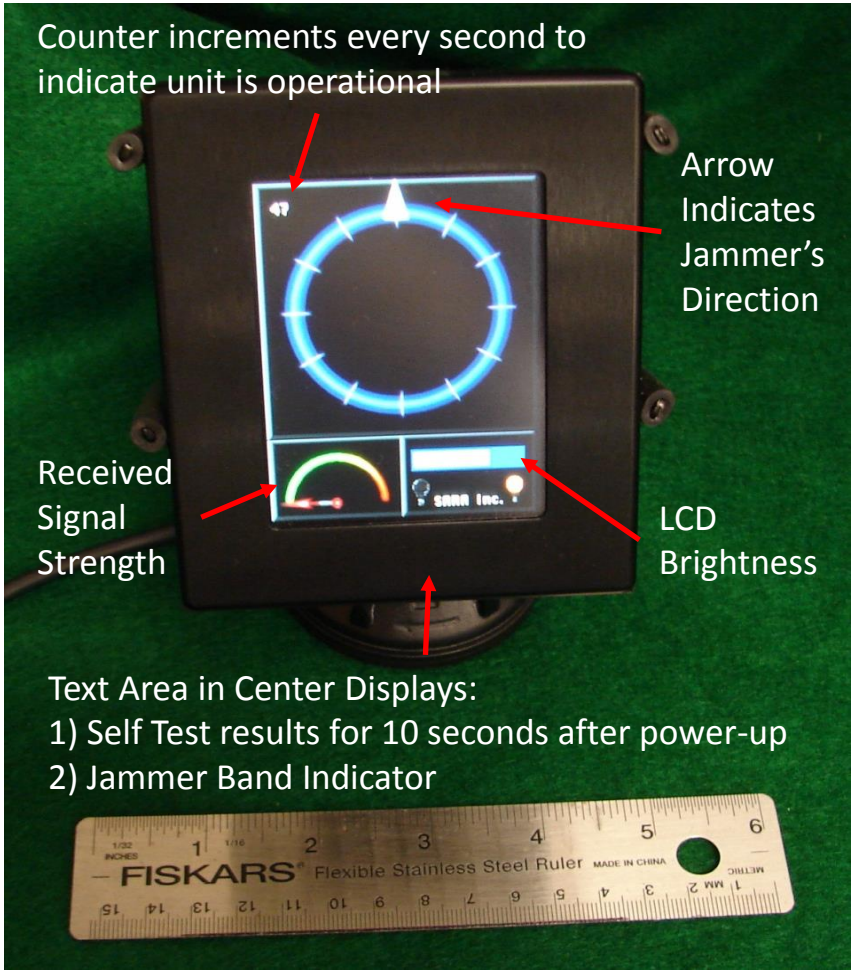
JLOC HTML and GIS Capabilities



Homeland Security

HammerHead Jammer Locator





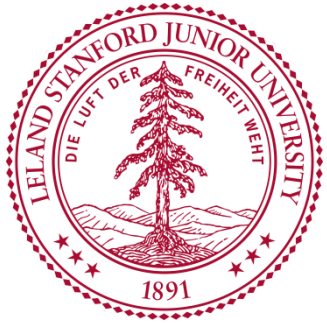
LCD user display provides Jammer direction and received signal strength information

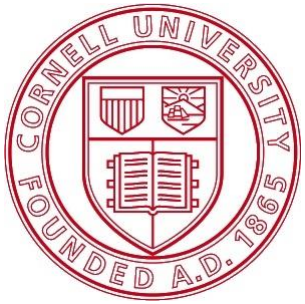
Homeland Security

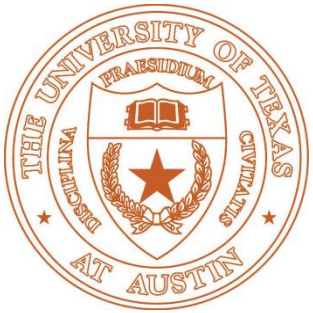
NIST and AMC Timing Experiment

- Test between NIST, Boulder and Alternate Master Clock (AMC), Schriever, AFB
- CenturyLink provides three different circuits to carry the timing signals
- Symmetricom provides PTP timing signals over Gigabit Ethernet
- Sending PTP signals over long distances directly from a UTC source requires further testing
- Testing to commence Fall 2013, few months of data collection

Collaboration Through Teamwork







Homeland Security

THANK YOU

FOR MORE INFORMATION

John.Merrill@hq.dhs.gov

(202) 447-3731 PNT PMO

(202) 731-9628 Mobile

Homeland Security

Backup Slides

ENFORCEMENT BUREAU
SIGNAL JAMMER ENFORCEMENT INITIATIVE

Legal Framework

Jammers disrupt critical public safety communications, placing first responders like law enforcement and fire fighting personnel at great risk. In addition, jammers can prevent 9-1-1 and other emergency phone calls from getting through when help is needed the most.

Broad Statutory Prohibition: The Communications Act prohibits the operation, manufacture, importation, marketing, and sale of signal jamming devices and other equipment designed to block, jam, or otherwise interfere with authorized radio communications (e.g., GPS, cell phone, Wi-Fi, and radar communications).

- **47 U.S.C. § 301: requires a valid FCC authorization or license for the operation of radio transmitting equipment. Signal jamming equipment cannot be authorized or licensed, however, because its purpose is to interfere with radio communications in contravention of Section 333.**
- **47 U.S.C. § 302a(b): prohibits the manufacture, importation, marketing, sale, or operation of jamming devices within the United States.**
- **47 U.S.C. § 333: prohibits willful or malicious interference with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government.**

Operating a jammer violates Sections 301, 302(b), and 333 of the Act.
Manufacturing, importing, marketing, or selling a jammer violates Section 302(b) of the Act.

Violations of the jamming prohibition can lead to substantial monetary penalties (up to $112,500 for any single act), seizure of the illegal jammer, and criminal sanctions including imprisonment.

Homeland Security

Recent Enforcement Actions

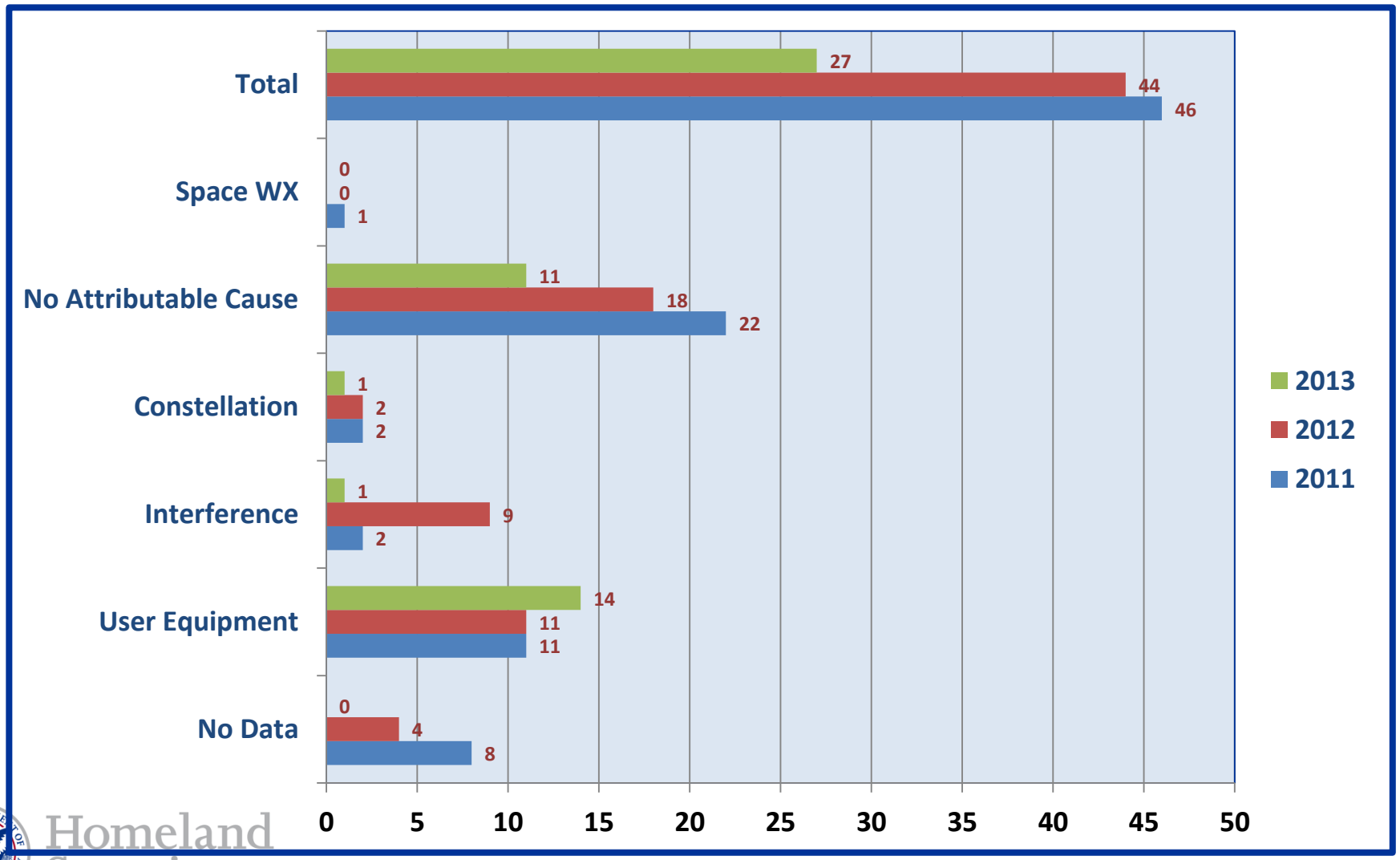
FCC jammer enforcement has been substantially more aggressive this year than in the past, including first-ever proposed monetary penalties for jammer use by an individual.

- **Taylor Oilfield and Supply Room**
  - **Notices of Apparent Liability for Forfeiture and Orders (NALs) released on April 9, 2013—**

    one to The Supply Room, Inc. and the other to Taylor Oilfield Manufacturing, Inc. The NALs proposed forfeitures totaling $270,000 for operating multiple cellphone jamming devices, and also found that the two entities illegally imported jamming devices.
  - **The penalty reflects upward adjustments based on the harm to public safety and duration of use, and a downward adjustment for voluntary relinquishment.**
- **Gary P. Bojczak – First-ever penalty proposed for an individual using a jammer**
  - **NAL released on Aug. 2, 2013, proposed a $31,875 forfeiture for operating a GPS jammer.**
  - **In response to an FAA complaint, an agent from the FCC's New York Office found that signals emanating from a vehicle driven by Mr. Bojczak were interfering with a "ground based augmentation system" (an enhanced navigation system) in pre-deployment testing at Newark airport.**
  - **The penalty reflects upward adjustments based on the harm to public safety, and a downward adjustment for voluntary relinquishment.**
- **The Enforcement Bureau also has numerous other ongoing investigations.**

USCG NAVCEN GPS Outage Reports

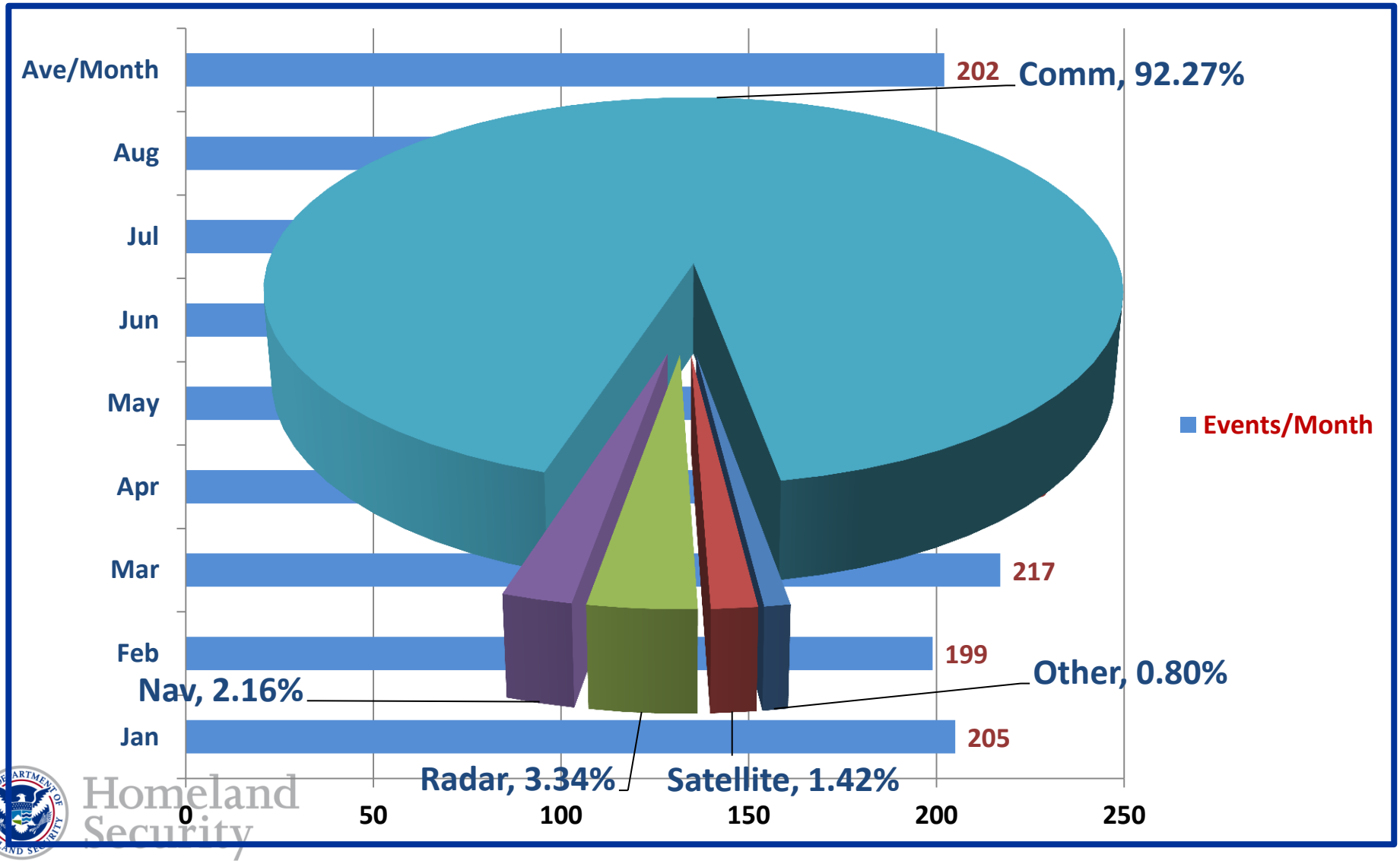
Source: August 2013 USCG NAVCEN



Homeland Security

2013 FAA RFI Events by Month

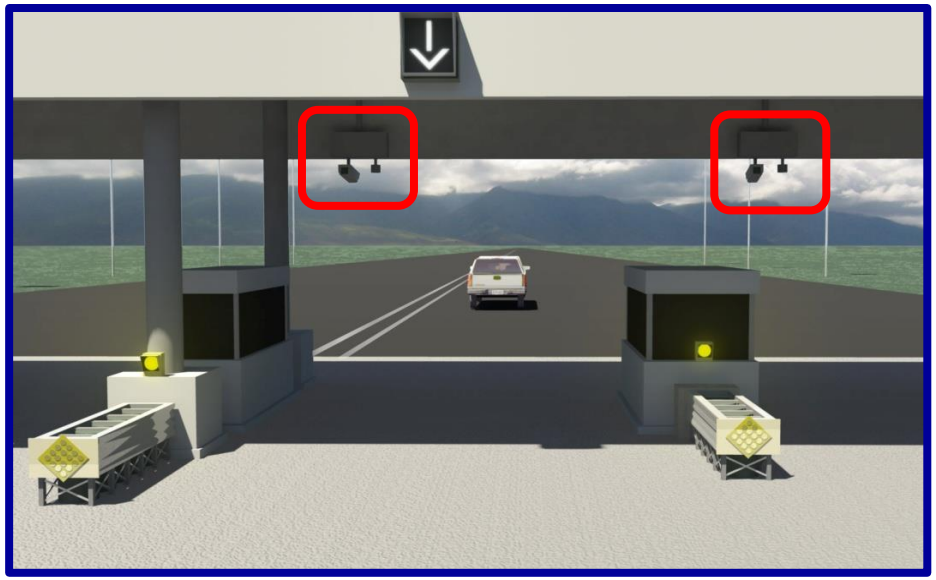
Source: August 2013 FAA Spectrum Engineering Office

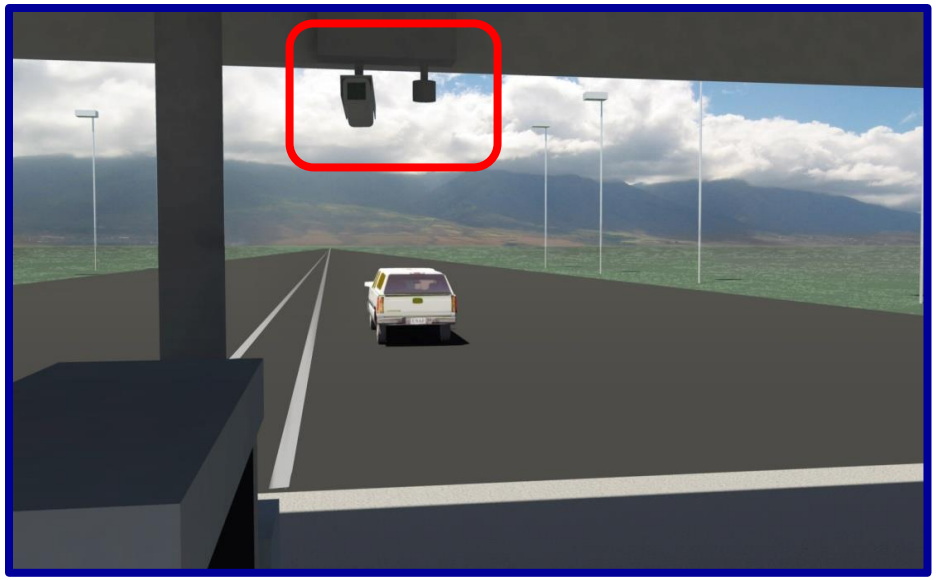


Homeland Security

Port Of Entry Concept

Source: Air Force Research Lab

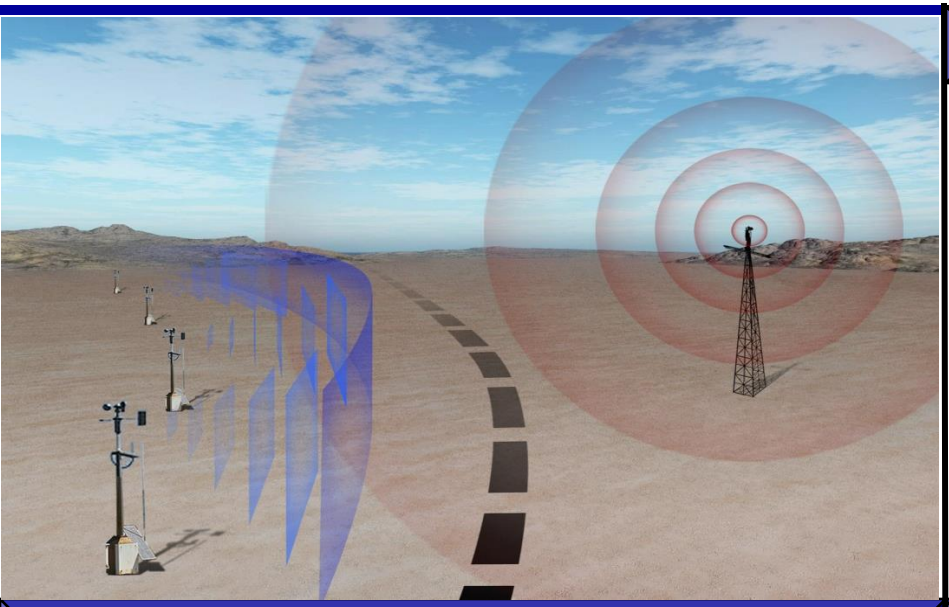




- **Jammer Detection Integrated with Camera System**
- **Alert Enforcement Personnel to Jammer Presence**
- **Detect & Track Jammers Approaching Entry Point**
- **Multi-Lane Distinction**
- **UNITRAC Database Connection**

Homeland Security

Perimeter Watch Concept



Description

- Static mounted array of sensors along a border
- Persistent monitoring of jamming activity
- Simultaneously monitors, detects and precisely geo-locates multiple GPS/Comm Jammers
- Covert – includes weather monitor station
- Net enable via data link or hard line

Program Goals

- Deliver operational capability to the user
- Produce a fully field operable, highly accurate GPS jammer geo-location capability
- Static mount installation
- Small, light weight, low power, upgradeable

Benefits to the User

- Persistent monitoring, detection, geo-location and reporting of GPS and Comm jammer activity; improves situational awareness
- Provides real time intelligence on jamming activity; near real time geo-location solution
- Remote automated notification of jammer presence, location, and movement

Homeland Security