



# DHS S&T First Responder Electronic Jamming Exercise

---

Briefing for NPSTC

**September 28, 2016**

**Sridhar Kowdley**

Program Manager  
First Responders Group  
Science and Technology Directorate



**Homeland  
Security**

Science and Technology

# Exercise Overview

- **Purpose:** Conduct live testing and demonstrations of first responder communications in a electronic jamming threat environment provided by White Sands Missile Range (WSMR)
- **Outcomes:** Understand the impact of electronic threats on first responder communications and mission operations; identify training gaps and mitigation strategies; and share lessons learned and best practices with first responders nationwide




**Homeland  
Security**


Science and Technology

# Electronic Jamming Threat

- First responders across the country face increased electronic jamming threats, notably jamming of GPS, radio and wireless systems
- Proliferation of electronic jammers can delay emergency response times, escalate hazardous situations, result in loss of life or facilitate illicit activities
- In addition to first responder threats, this exercise will address additional threats to homeland security, including:
  - Global War on Terror**
  - Southern Border Protection**
  - Infrastructure Protection and Security**



## Cellular, GPS, Wi-Fi, and Other Signal Jammers



Signal jammers are illegal and can interfere with operational channels commonly used by first responders, disrupting vital communications or affecting emergency operations. There have been documented incidents of the loss of first responder radio communications near areas where cell and GPS jammers were being used. Loss of cellular coverage was also observed in these areas which prevented 9-1-1 and other emergency calls from being made. Jammers can target cellular, GPS, Wi-Fi, and other radio signals, individually or in combination.

**Indicators of Jamming:**

Disruption or failure of wireless communications or mapping equipment, including cellular or GPS devices, for unknown reasons could indicate interference by a jammer.

**Specific indicators might include:**

- Inability to transmit or receive on two-way radios outside of known "dead zones."
- Unusual sounds on designated frequencies, such as white noise, intermittent electronic chirping, or tones.
- Lack of normal sounds heard on designated frequencies or presence of "dead air."
- Technical difficulties that appear and disappear intermittently.
- Lack of audible click when keying microphone.
- Abrupt loss of communications, especially if stationary.
- Loss of lock, intermittent disruption, or general failure of a GPS receiver or GPS-enabled device.

**Actions:**

Incidents where a suspect operating a jammer is identified should be reported to the FCC at [www.fcc.gov/complaints](http://www.fcc.gov/complaints) or 1-888-CALL-FCC (1-888-225-5322). The FCC will investigate and take follow-up administrative enforcement action against the subject where applicable.

**Reports should include the following:**

For an ongoing incident or if a suspect is identified, provide:


- Identification details of suspect using illegal equipment (Name, DOB, vehicle tag, etc.).
- Description or identification of suspected jamming device (including photo if available).

For all incidents, provide:

- Reporting party's name/contact information/agency, date, time, duration, location, & affected mission or operations.
- Nature of the disruption (such as single occurrence, recurring, intermittent, or loss of signal indication).
- Equipment affected (type, model, application).
- Environmental conditions (weather, topography, terrain, time of day).
- Steps taken to improve or regain ability to use equipment.
- Other wireless devices not affected by the suspected jamming or anomaly.

The FCC can assist with legal and technical questions when jammers are encountered or suspected. Contact points are through [jammerinfo@fcc.gov](mailto:jammerinfo@fcc.gov) or the FCC's Spectrum Enforcement Division at (202) 418-1160 (9 AM - 5 PM ET) or 1-888-CALL-FCC. Additional public information is available at: <http://www.fcc.gov/jammers>

**Jammer Examples (including disguised devices)**



**Applicable Laws:**

Federal laws prohibit any person from willfully or maliciously interfering with authorized radio communications and prohibit the manufacture, sale, marketing, importation, distribution, or shipment of jamming equipment.

State laws may also prohibit the possession or certain uses of jammers (e.g., interference to police communications) and thus provide a basis for local seizure and prosecution. Law enforcement agencies should develop a strategy in advance with their office of legal counsel.

**The Communications Act of 1934**

**Section 301** - requires persons operating or using radio transmitters to be licensed or authorized under the Commission's rules (47 U.S.C. § 301).

**Section 302(b)** - prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States (47 U.S.C. § 302a(b)).

**Section 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 (47 U.S.C. § 333).

**Section 503** - allows the FCC to impose forfeitures for willful or repeated violations of the Communications Act, the Commission's rules, regulations, or related orders, as well as for violations of the terms and conditions of any license, certificate, or other Commission authorization, among other things (47 U.S.C. § 503).

**Section 510** - allows for seizure of equipment used, possessed, advertised, or sold with knowing intent to violate Sections 301 or 302 (47 U.S.C. § 510).

**FCC Rules**

**Section 2.803** - prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States (47 C.F.R. § 2.803).

**Section 2.807** - provides for certain limited exceptions, such as the sale to U.S. government for authorized, official use (47 C.F.R. § 2.807).

**The Criminal Code (Enforced by the Department of Justice)**

**Title 18, Section 1362** - prohibits willful or malicious interference to U.S. government communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1362).

**Title 18, Section 1367(a)** - prohibits intentional or malicious interference to satellite communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1367(a)).

In 2015, DHS issued a joint bulletin with the FCC capturing the impact of jamming on First Responder Communication and emergency communications.



**Homeland Security**

Science and Technology

# So What did We Do?

- Coordinated with DHS OEC and DHS components to identify participants
- Worked with FCC/NIST and DHS to obtain jammers
- Contracted with AF 746 TS to conduct testing and operate jammers
- Conducted detailed planning sessions (spectrum/scenario)
- Obtained and characterized jammers
- Obtained invitational travel for state and local first responders

## Exercise Resources

- Over 225 personnel participated on-site
- Over 500 personnel supported planning
- 61 organizations supported exercises
- 16 mobile command and first responder vehicles
- 70 first responder scenarios conducted
- 53 commercial and DOD jammers
- Operated over 500 square miles of desert – more than 7 times the size of Washington, D.C.



**Homeland  
Security**

Science and Technology



U.S. Immigration and Customs Enforcement



U.S. Customs and Border Protection



FEMA



# Homeland Security



DIGITAL GLOBAL SYSTEMS

MITRE



SwRI



Science and Technology



GD



U.S. AIR FORCE



STARK AEROSPACE

LOCKHEED MARTIN

HARRIS

# First Responder Vehicles



**Homeland  
Security**

Science and Technology

# Day 1: Jamming Critical Infrastructure

- Participants included the Department of Defense, Federal Communications Commission, Federally-Funded Research and Development Centers, and industry partners
- Tested GPS and anti-jamming GPS systems against a variety of GPS jamming threats



**Homeland  
Security**

Science and Technology

# Day 2: Jamming UAS

- Participants included Lockheed Martin Aerospace, Stark Aerospace, AeroVironment, Air Robot, and Stanford University (not part of RAPS)
- Tested fixed and rotary wing unmanned aircraft systems (UAS) against GPS and broadband jamming to examine the effect on navigations and communications capabilities
- Stanford University tested a UAS platform that autonomously locates GPS jammers by honing in on the jammer's signal – and it was successful!
- The other four vendors tested their UAS's to locate suspects during drug smuggling and illegal immigration scenarios, assessed by officers from the U.S. Border Patrol







# Day 3-5: Jamming First Responders

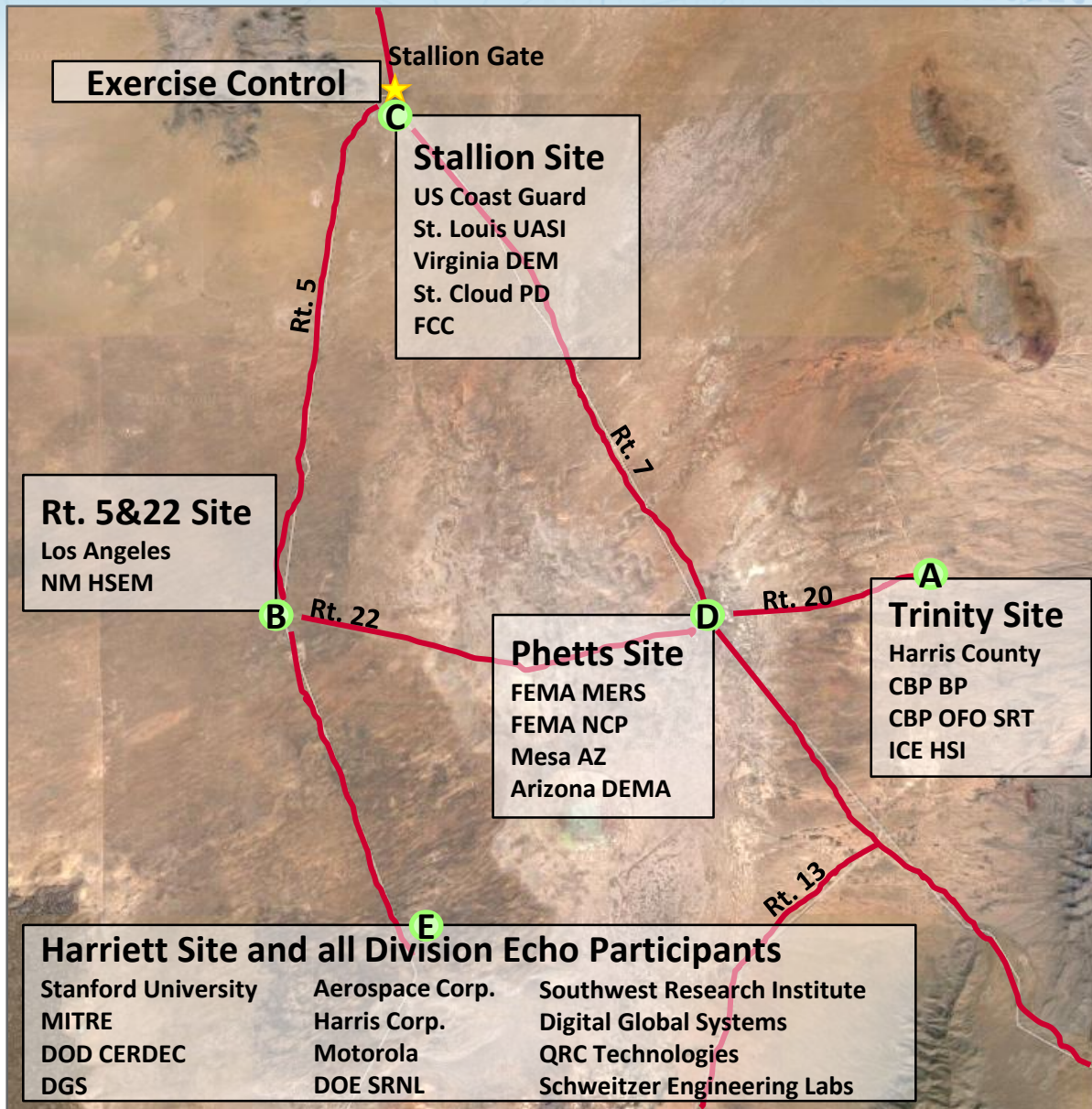
- Participants included Los Angeles County Sheriff's Department, the Harris County (TX) Fire Marshall's Office, the Mesa (AZ) Police Department, New Mexico Department of Homeland Security and Emergency Management, FEMA, ICE, CBP, USCG, and industry
- Tested first responder communications systems, including land mobile radio systems (multiple bands), Cellular, Wi-Fi, Satellite, GPS, Bluetooth, and other wireless devices (i.e. thermal imaging)
- Assessed not only how the equipment was impacted by GPS and broadband jamming, but also how well responders were able to work around the jamming to still accomplish their mission



**Homeland  
Security**

Science and Technology

# Day 3-5: Exercise Layout At WSMR



## Organization

By splitting up into four first responder divisions and one industry division, we were able to run 5 simultaneous scenarios with different jammers – **more than 70 scenarios over three days**

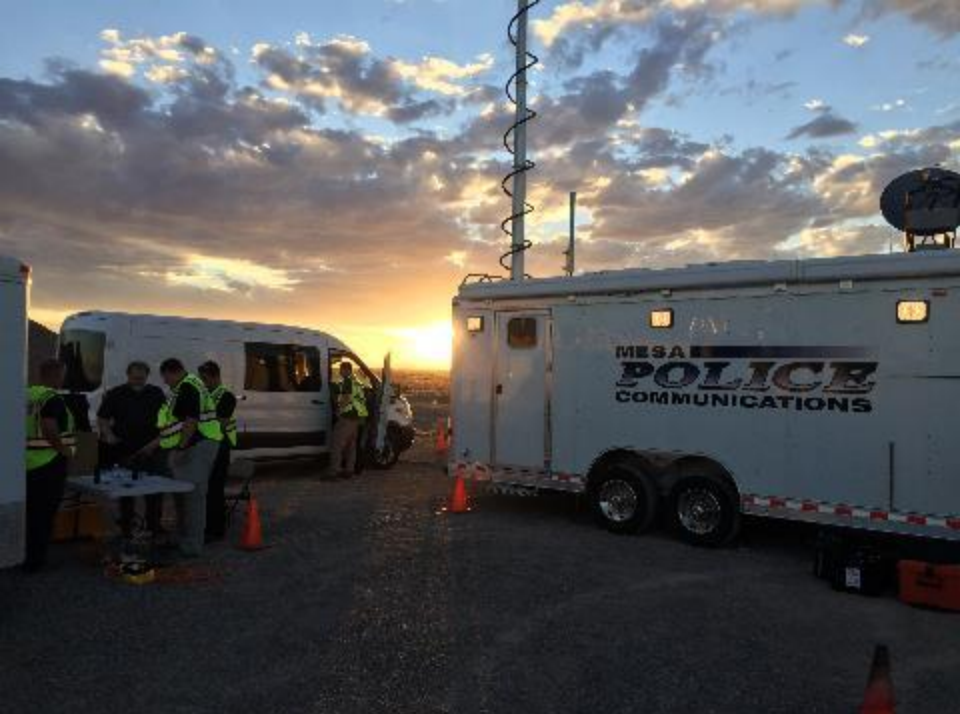
## Industry Testing

Industry participants at Division Echo tested a variety of receivers, spectrum analyzers, and communications devices against the full range of jammers, and have shared their data with DHS S&T for analysis



















# Initial Observations and Findings

- First Responders were all surprised at how these commercial jammers worked
- First Responders recognized that they have gaps in training, and stated they would “have to rethink their communications plans” and identify mitigation strategies
  - A representative from FLETC witnessed test and we will be discussing anti-jamming training.
  - A responder from the Arizona Department of Emergency Management and Military Affairs said that he is now “ten times more likely to recognize intentional jamming” than before the exercise
- Detailed reports and test results will be compiled from data provided by all organizations and data collected in the field
  - Reports containing vulnerabilities appropriately classified, including FOUO/LES planned for October 2016
- Responders used creative problem-solving to accomplish their mission in jamming environments



**Homeland  
Security**

Science and Technology

# Acknowledgements

- This exercise would not have been possible without significant contributions from:
  - **DHS Office of Emergency Communications** for coordinating with State and Local participants and assisting with exercise execution
  - **New Mexico Department of Homeland Security and Emergency Management** for providing assets and supporting exercise execution
  - **FCC and FAA** for assisting in spectrum authorization and coordinating with DOD to characterize jammers
  - **Air Force 746 Test Squadron and White Sands Missile Range** for supporting exercise planning, providing the test environment, and supporting exercise execution including operating commercial and DOD jammers and facilitating logistics



# Follow-On Exercise in 2017

- Objectives:
  - Test anti-jamming mitigation technologies in a field setting
  - Evaluate first responder jamming mitigation techniques, tactics and procedures (TTPs)
- Details:
  - Location and Date TBD
    - Looking at August-December 2017, depending on facility availability
    - Evaluating DOD and non-DOD facilities
  - Similar scope in size— 200-300 participants
  - Split into two parts – a T&E event to technically evaluate the mitigation technologies and a full-scale exercise to evaluate the first responder TTPs
    - Each part will have different requirements for planning and execution
    - NUSTL will lead the T&E event with the industry participants
    - OEC and FEMA will help lead the exercise portion with first responders





# Homeland Security

---

Science and Technology