DHS SCIENCE AND TECHNOLOGY

Ensuring Resilient Communications

BRIEFING FOR POSITION, NAVIGATION & TIMING ADVISORY BOARD

May 17, 2018

Homeland Security
Science and Technology

John Merrill

Director
Office for Interoperability & Compatibility

First Responders Group

Science and Technology Directorate

Jamming 101: What is It?

- Jamming devices emit radio frequency signals – noise – over specific bands to overpower the intended signals
- Jammers are often cheaply manufactured overseas and are low-quality electronics, which means that they often emit inconsistent signals, making them hard to detect
- Jammers are mostly designed for overseas commercial markets to target GPS, cell phones, Land Mobile Radio systems, Wi-Fi, Bluetooth and other frequency-transmitting devices

Jamming 101: Legal Review

- **Manufacture**, **importation**, **marketing**, **sale** or **operation** of jamming devices is **ILLEGAL** in the United States (47 U.S.C. § 302a(B))
- It is also **ILLEGAL** to interfere with any licensed radio communications authorized by the FCC or operated by the U.S. Government (47 U.S.C. § 333)
- Interfering with federal communications falls under the NTIA, rather than the FCC
- **Talk with your legal counsel about legal authorities available to your agency**
  - As appropriate, jamming incidents may be prosecuted as **interfering with police business** or as a **cybercrime**, in addition to jamming-specific charges

Jamming 101: Threats and Motives

- Jammers are often used **maliciously** to mask a crime, such as burglary, vehicle theft, cargo theft, parole violations, drug/human trafficking or acts of terrorism
- Jamming may also be used in cases without underlying criminal intent. Examples of **nuisance** jamming include:
  - Mobile GPS jammers used by drivers evading GPS tracking and speed monitoring
  - Cellular or Wi-Fi jammers used to establish “quiet zones” free of electronic distractions in churches, restaurants, commuter rail and workplaces
- Jamming presents additional threats to homeland security, including potential uses against the officers and technologies guarding the southern border and critical infrastructure targets

Jamming 101: Mission Impacts

- Communications are a lifeline for first responders and federal law enforcement
- More than radios and phones rely on secure communications.
- Jammers could impact:
  - Fire department mayday transmissions
  - Hazmat detectors
  - Air support
  - Backup calls to dispatch
  - Alarm systems
  - Remote control robots
  - K-9 law enforcement response
  - Unmanned Aircraft Systems units
  - On-body or environmental sensors
  - Video and photo transmission
- In addition to communications, **jamming could impact position, navigation and timing systems used in critical infrastructure**

DHS Goals for Resilient Communications

1. **Improve communications resiliency** to jamming and other interference threats to increase federal, state and local capabilities to **recognize, respond to, report and resolve** interference incidents
2. Better **understand the spectrum threat environment** and critical infrastructure vulnerabilities to interference to **inform risk-based policy**, acquisition, training and R&D decisions and investments
3. **Improve jammer interdiction and enforcement** to reduce number of jammers in circulation and deter future purchases and use

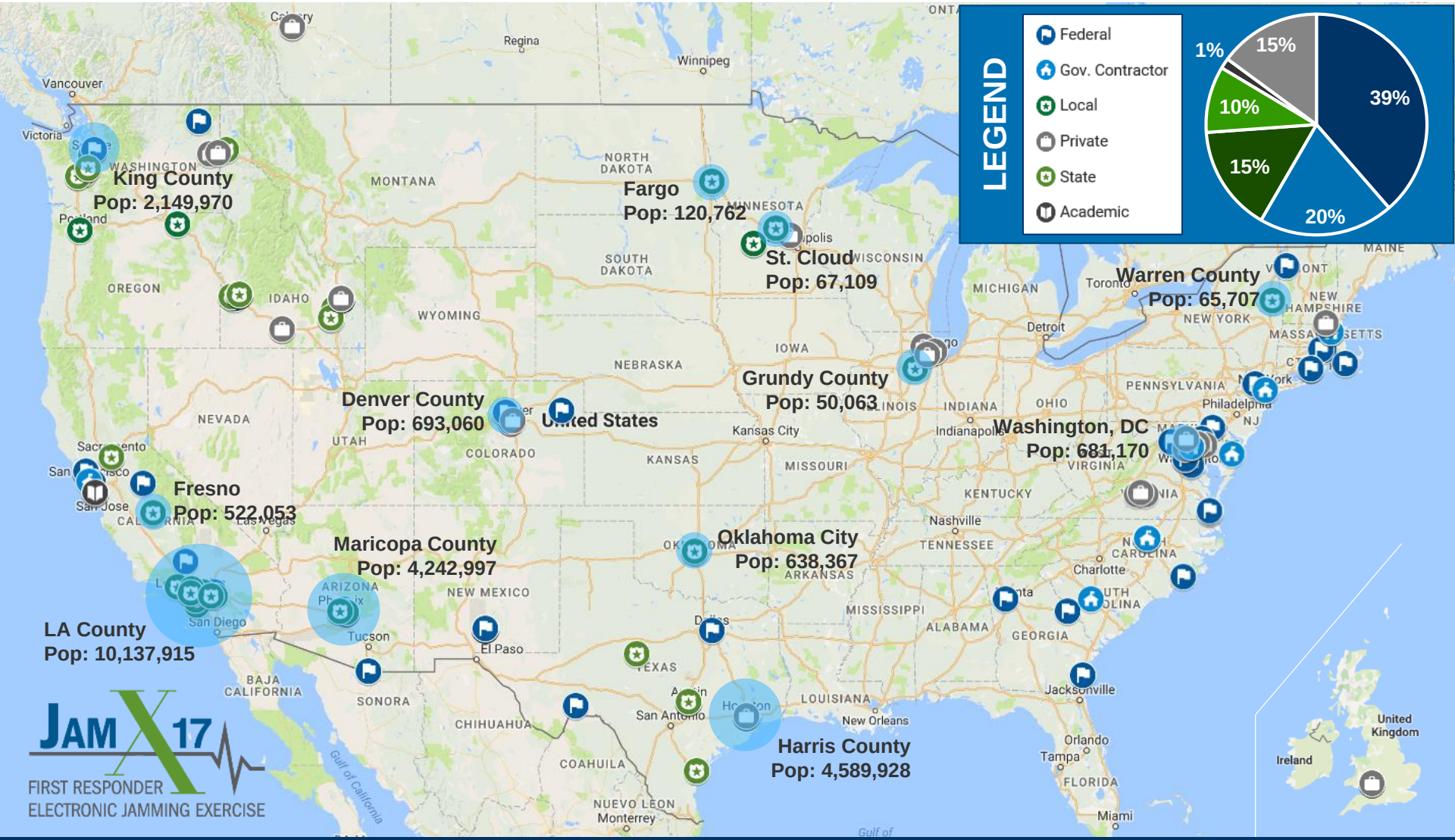
DHS S&T Work

- **2016 First Responder Electronic Jamming Exercise** – July 2016
  - **Purpose**: Test first responder and federal communications gear and UAS against illegal, commercial-grade jammers to identify impacts and validate mission risks
  - **Outcomes**: Identified clear vulnerabilities and mission impacts, made initial recommendations
- **2017 First Responder Electronic Jamming Exercise (JamX 17)** – July 2017
  - **Purpose**: Assess technologies and tactics that help responders and federal LE to identify, locate and mitigate the impact of illegal, commercial-grade jamming
  - **Outcomes**: Refined recommendations and will be developing a Resilient Communications Toolkit to help federal agencies and responder organizations raise awareness of jamming threats, assess interference risks, and train personnel to identify, locate and mitigate threats
- **GPS Equipment Testing for Critical Infrastructure (GET-CI)** – September 2017
  - **Purpose**: Allow critical infrastructure equipment vendors the opportunity to experience hostile GPS scenarios
  - **Outcomes**: Improved vendor awareness of threats and vulnerabilities; motivated vendors to develop and test mitigations (GET-CI 2018) and to participate in resiliency compliance program

JamX 17 Results

- **Overall**:
  - A very successful event with participation from 260 primary participants, and an additional 29 VIPs – **all participants benefitted from participation** and were able to collect data to understand impact of illegal, commercial-grade jammers
- **Jammer Characterization**:
  - Impact zones varied, but ranged from 0-200 meters
- **Tactics to Identify, Locate and Mitigate**:
  - Initial results suggest that **several of the tactics were successful** at mitigating the impact of jamming under specific conditions
  - Final results will be used to create best practices and training materials
- **Technologies to Identify, Locate and Mitigate**:
  - Several vendor participants were successful, and many **identified areas for improvement** based on the data gathered during the exercise
- **Feedback from Participants**:
  - Participant from the State of Washington said commercial partner, Sprint, **"got $1 million worth of data"** over the two days that the team participated
  - DTR, Inc., who tested a mitigation solution during JamX 17, said they had to **"rethink their entire approach to implementation"**
  - Participant from Grundy County (IL) 9-1-1 said, "**the experience was priceless"**

JamX 17 Participants Across America



Local responder agencies at JamX 17 represented nearly **24 million Americans**

JamX 17 Jammer Effectiveness

- DHS S&T used illegal, commercial-grade, non-intelligent GPS and communications band jammers at JamX 17, which were purchased through a law enforcement investigation
- Commercial bands were more vulnerable to these jammers than public safety bands
- Jammer effectiveness was generally limited to short ranges
- Many jammers degraded in performance over time, emitting less precise frequencies and at varying power levels
- Effectiveness of jammers is consistent with their power-levels: **the higher the transmit power, the more effective**
- Tactics and technologies may be employed to identify, locate and mitigate the effects of jammers
- For more detailed results, email Jamming.Exercise@hq.dhs.gov

JamX 17 GPS Observations

- DHS S&T had 12 industry participants at JamX 17, 10 of which tested GPS systems
- Performance of individual GPS receivers and antennas varied when jammed
  - Antenna and receiver design for different GPS devices showed that **some GPS receivers were more resistant to jamming than others**
  - Jammer antenna patterns are possible reason for their lack of effectiveness
- DHS S&T recommends further investigation of jammer signal structure and a detailed study of performance impact using different antennas on jammers

Examples of GPS Systems Tested

NovAtel GPS Anti-Jam Technology (GAJT)

MITRE Anti-Jam Sleeve

Chronos JammerCam

USCG GPS Receivers

CRFS Spectrum Monitoring Vehicle

THEIF Direction-Finding Tool

Effectiveness of Commercial Jammers in GPS Bands at JamX 17

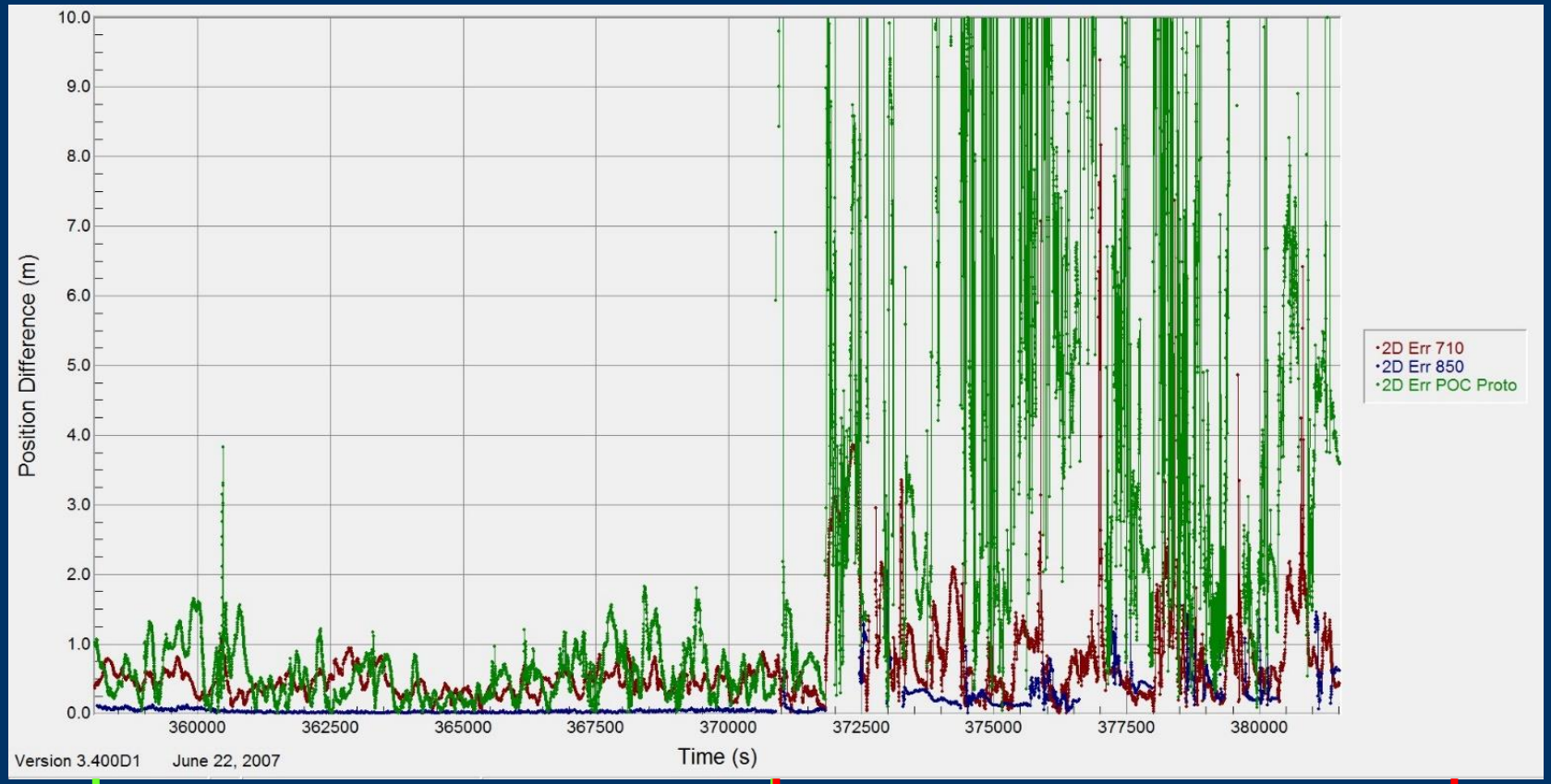
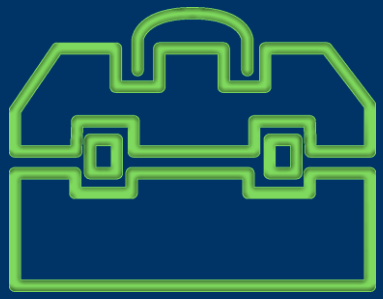


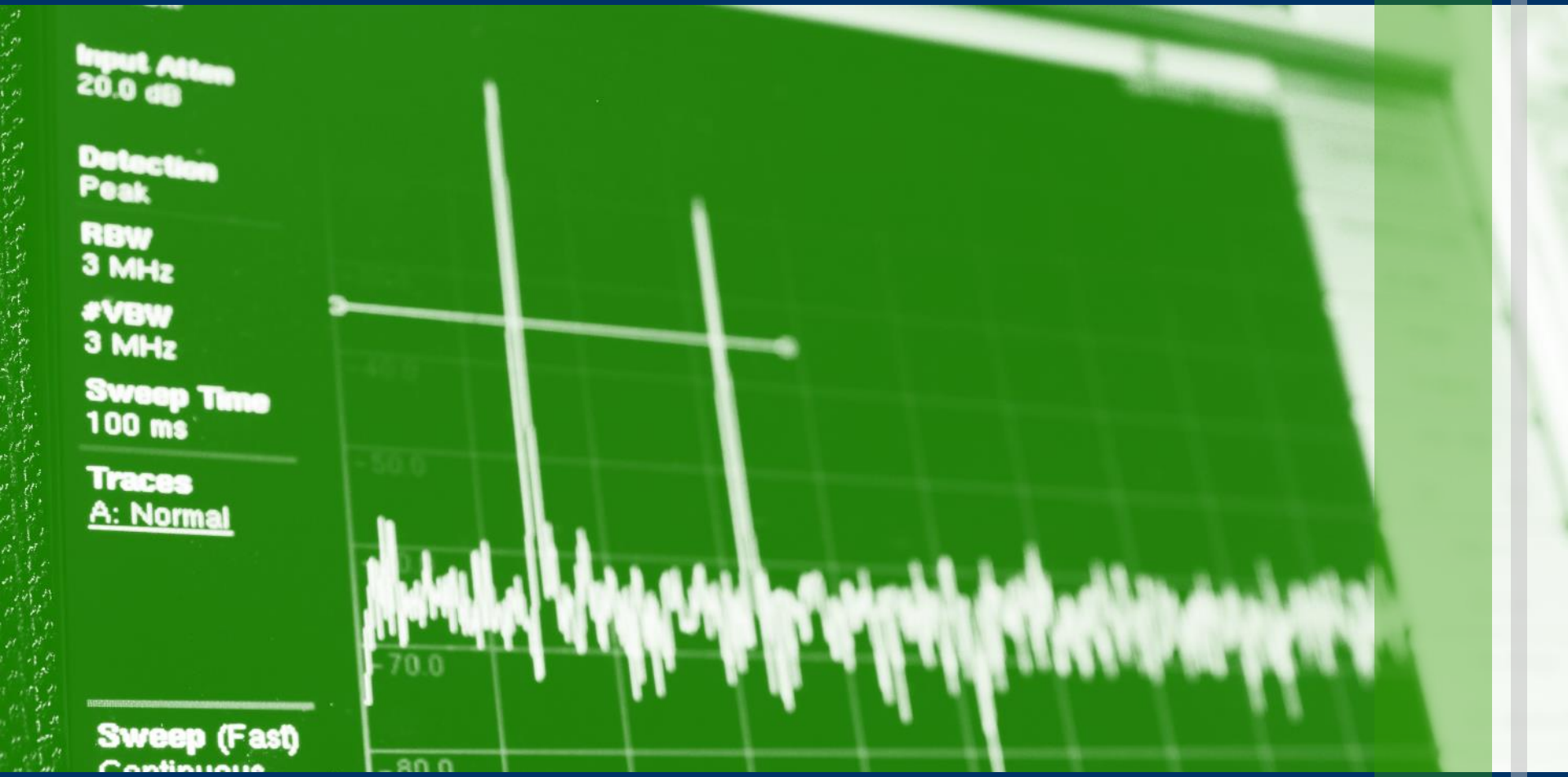
**Image Courtesy of NovAtel*

What's Next: Expanding Impact

- DHS S&T is working with the DHS Office of Emergency Communications to develop a **Resilient Communications Toolkit** for federal agencies and communities nationwide
  - Toolkits will include materials to help raise awareness of jamming threats, assess interference risks, and train responders to identify, locate and mitigate jamming threats



- DHS hopes to pilot the Toolkit with major cities and federal agencies in Winter 2019, and expand thereafter
- DHS S&T is looking for partner agencies to pilot initiatives – email **Jamming.Exercise@hq.dhs.gov** to discuss further
- DHS S&T will host **JamX 19** next:
  - Objectives: evaluate how well communications resiliency recommendations were implemented during pilots, assess advancements in counter-jamming technologies, profile non-jamming interference sources and provide an interference testbed for industry
  - Date and location: TBD



INITIAL RECOMMENDATIONS

Preparing Agencies & Infrastructure

Education	Preparation	Evaluation

- **Educate operational employees** – Can they recognize a jammer? Do they know the symptoms of interference? Do they know how to respond to and report incidents? If they find jamming, do they check for other illegal activities?
- **Prepare employees and agency policies** – Ensure spectrum interference detection equipment is available and personnel are trained to use it. Update agency policies on reporting requirements. Review communications and IT policies for best practices. Conduct readiness exercises that include communication outage scenarios.
- **Evaluate communications resilience** – Assess baseline communications vulnerabilities and address gaps. Evaluate how well employees are prepared to identify, locate and mitigate interference during regular exercises. Develop after action reports to review how interference incidents were handled and identify lessons learned to incorporate throughout the agency.

Mitigating Jamming:
Operator Perspective

- Communications failures are always assumed to be equipment issues – double check
- Education is key – operators must understand and recognize jamming threats to take them seriously
- Basic mitigation strategies for operators:

Switch Comms
Use a different device or band if one stops working

Move it
Try moving 10-20 feet to improve coverage

Go High
Elevate your radio or antenna where possible

Mobiles vs Portables
Use portables to receive and mobiles to transmit

Shield Yourself
Move behind a car or building to block signals

Cover the Jammer
Once located, cover with a mylar emergency blanket

Mitigating Jamming:
Increasing Communications Resiliency

- Ensure all levels of organization are aware of jamming threats
- Consult organization's legal counsel to understand state and local jamming laws
- Encourage regular radio training drills for operational personnel
- Have communications systems in multiple bands for backup
- Require prompt reporting of "equipment issues" to the communications team
- Switch on Automatic Gain Control in radio programing for all LMRs

Mitigating Jamming:
Special Events

- Develop a PACE (Primary, Alternate, Contingency, Emergency) plan for communications
- Alert coordinating jurisdictions of potential jamming threats, symptoms and reporting procedures
- Train event security teams on jammer identification and mitigation tactics
- Monitor event with spectrum analyzers
- Use direction-finding tools to locate interference sources

Get Involved and Get Prepared

- Everyone has a responsibility for communications resiliency
- Raise awareness of jamming threats
- Implement DHS S&T recommendations to boost your communications resiliency
- Have a plan for what operators do when they suspect interference
- Talk to your legal counsel about applicable jamming laws
- If you See Something, Say Something - Report all suspected jamming incidents to the FCC and/or local law enforcement

Engage With Us!

DHS S&T JAMMING EXERCISE PROGRAM

EMAIL
Jamming.Exercise@hq.dhs.gov

TWITTER
@dhsscitech

WEBSITE
www.DHS.gov/NGFR

FACEBOOK
@FirstRespondersGroup

Homeland Security

Science and Technology