DHS SCIENCE AND TECHNOLOGY

Briefing for NPSTC

2017 FIRST RESPONDER ELECTRONIC JAMMING EXERCISE

September 6, 2017

Homeland Security
Science and Technology

Sridhar Kowdley
Program Manager
First Responders Group
Science and Technology Directorate

What is Jamming?

- Jamming devices emit radio frequency signals at specific bands with the intention of overpowering other signals
  - For example, a GPS jammer will emit “noise” in GPS frequency bands, which overwhelms the GPS receiver, blocking all of the legitimate satellite signals from getting through
- A communication system is “jammed” when the noise has significantly degraded or blocked the desired signal

Interference Symptoms

Disruption or failure of wireless communications or mapping equipment – including cellular, LMR or GPS systems – for unknown reasons could indicated interference

You may be experiencing spectrum interference if you:

- Can't communicate in areas where you typically have good radio or cell coverage
- Can't communicate with normally reliable base radios or repeaters
- Can't communicate on multiple communications devices using multiple bands
- Notice a significant loss of lock or general failure of GPS systems
- Can significantly improve communications capability by moving a short distance away from a fixed "dead zone"

Jammers are Illegal

- Spectrum interference can have a **significant negative impact on the safety of American citizens** and the mission effectiveness of federal, state and local law enforcement and public safety organizations
  - **Jammers are both a criminal issue and a homeland security issue**
- **Manufacture**, **importation**, **marketing**, **sale** or **operation** of jamming devices is **ILLEGAL** in the U.S. (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)
- Per U.S. v. Rajib K. Mitra, **radio interference also constitutes violation of the Computer Fraud and Abuse Act** (CFAA) (18 U.S.C. § 1030)
  - This decision in April 2005 affirmed that **jamming constitutes a cybercrime** because the defendant caused "intentional interference with computer-related systems used in interstate commerce"
  - U.S. Sentencing Guidelines for cyber crimes suggest a **significant penalty for interference with critical infrastructure and public safety** (U.S.S.G. § 2B1.1(b)(18)(A)(iii) and (B))

DHS S&T Spectrum Resiliency Research

- Sridhar Kowdley (FRG OIC) leads the First Responder Electronic Jamming Exercise initiative, which focuses on conventional spectrum interference against public safety and law enforcement communications systems
- The 2016 and 2017 First Responder Electronic Jamming Exercises focused on illegal commercial-grade jammers that are bought online and illegally imported
  - Testing examined how jammers impact public safety communications systems and a first responder's ability to complete the mission
  - Impacted Bands: GPS, cellular, land mobile radio (federal, state and local frequencies), Wi-Fi, Bluetooth, over the air TV, etc.

FRG's Key Goals

- Help federal, state and local public safety and law enforcement recognize, respond to, report and resolve jamming incidents
- Better understand the volume and severity of the threat through increased awareness and analysis of reported jamming incidents
- End goal: **More resilient communications and critical infrastructure** for federal, state and local partners and greater understanding of spectrum threats
  - Homeland security starts with hometown security

2016 Exercise Overview

- **Problem**: DHS and the FCC are getting increased reports of jammer activity, but how could jammers impact or impede federal law enforcement and local public safety?
- **Approach**: In a live-jamming environment at White Sands Missile Range, DHS and participants tested:
  - First responder communications systems against commercial jamming;
  - Anti-jamming technologies against commercial jamming;
  - Unmanned Aircraft Systems (UAS) against complex GPS and commercial jamming; and
  - Fixed timing receivers (used in critical infrastructure) against complex GPS and commercial jamming.
- **Goals**: DHS S&T wanted to understand how severely illegal commercial-grade jammers impact public safety communications systems and mission response

2017 Exercise

- The 2016 Exercise defined how jamming can disrupt first responder communications; next, DHS **evaluated solutions to increase resiliency** during the 2017 First Responder Electronic Jamming Exercise (JamX 17)
- **Objective**: Fully characterize the impact of jammers and better enable first responders to **identify, locate and mitigate** the impact of jamming on public safety communications by evaluating **technologies** and **tactics**

JamX 17 Target Outcomes

At JamX 17, DHS gathered data and responder feedback on jammer impacts and the success of mitigation technologies and tactics. DHS is analyzing the data to **make, objective statistically relevant recommendations to the public safety community**

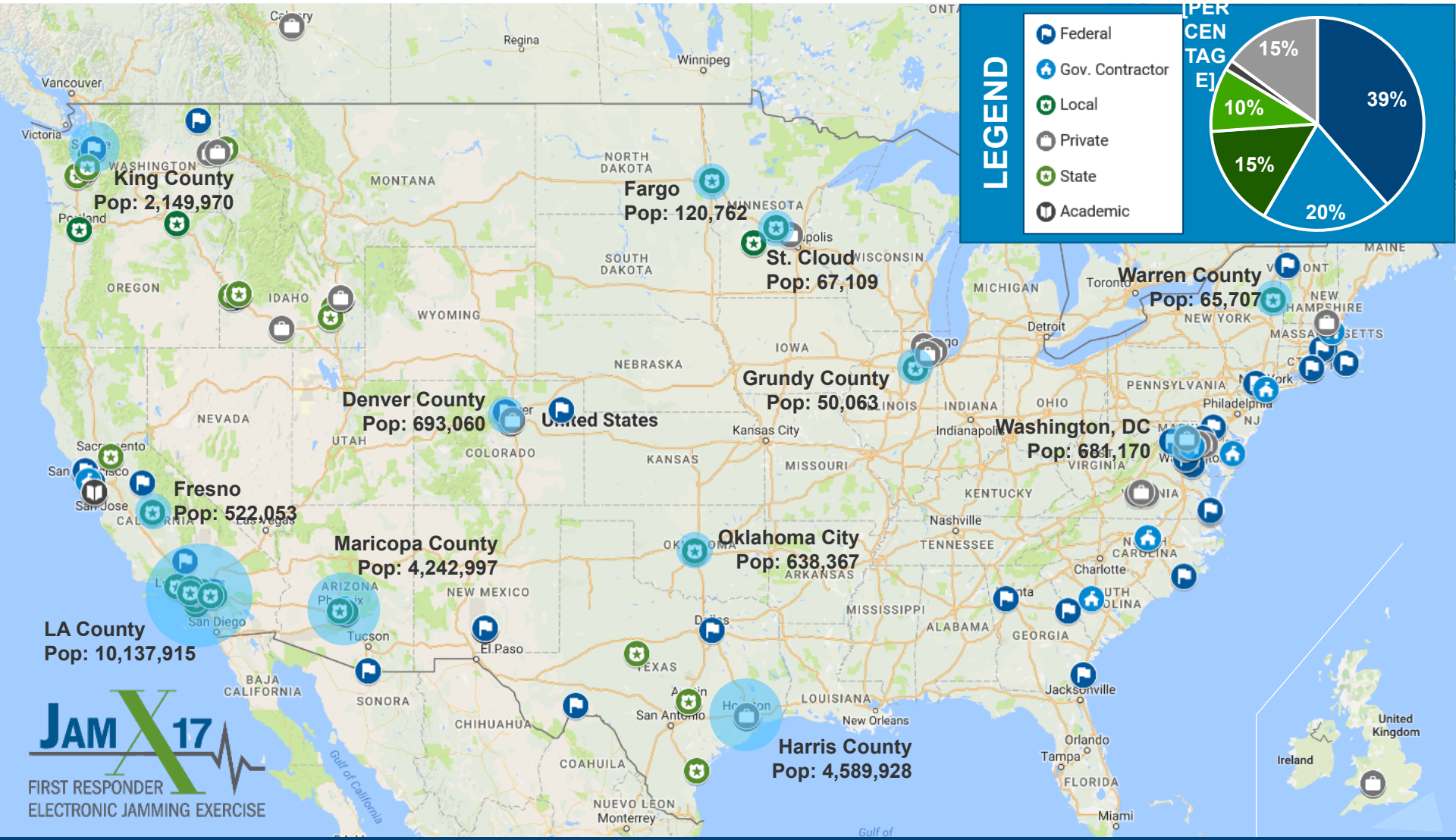
TARGET OUTCOMES

1. Develop **clear recommendations** about technologies and tactics that **improve resilience against jamming**
2. Design an **outreach and education campaign** to raise awareness of jamming threats and vulnerabilities, and **better prepare responders to recognize, respond to, report and resolve jamming incidents**
3. Propose a **training program** for federal and public safety organizations to help them **identify, locate and mitigate the impacts of jamming**
4. **Work with FEMA** to get jammer detection technology on the **Authorized Equipment List**

JamX 17 Initial 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 determined after analysis and 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** as well as the interaction with everyone"

JamX 17 Participants Across America



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

After Action Process

0 - 4 Months

1. Process Data
2. Analyze
3. Develop Conclusions
4. Align Technical Results to Operational Impacts

2 - 12 Months

1. Draft
2. Stakeholder Review
3. Security & ITAR Review
4. Finalize
5. Distribute

0 - 24 Months

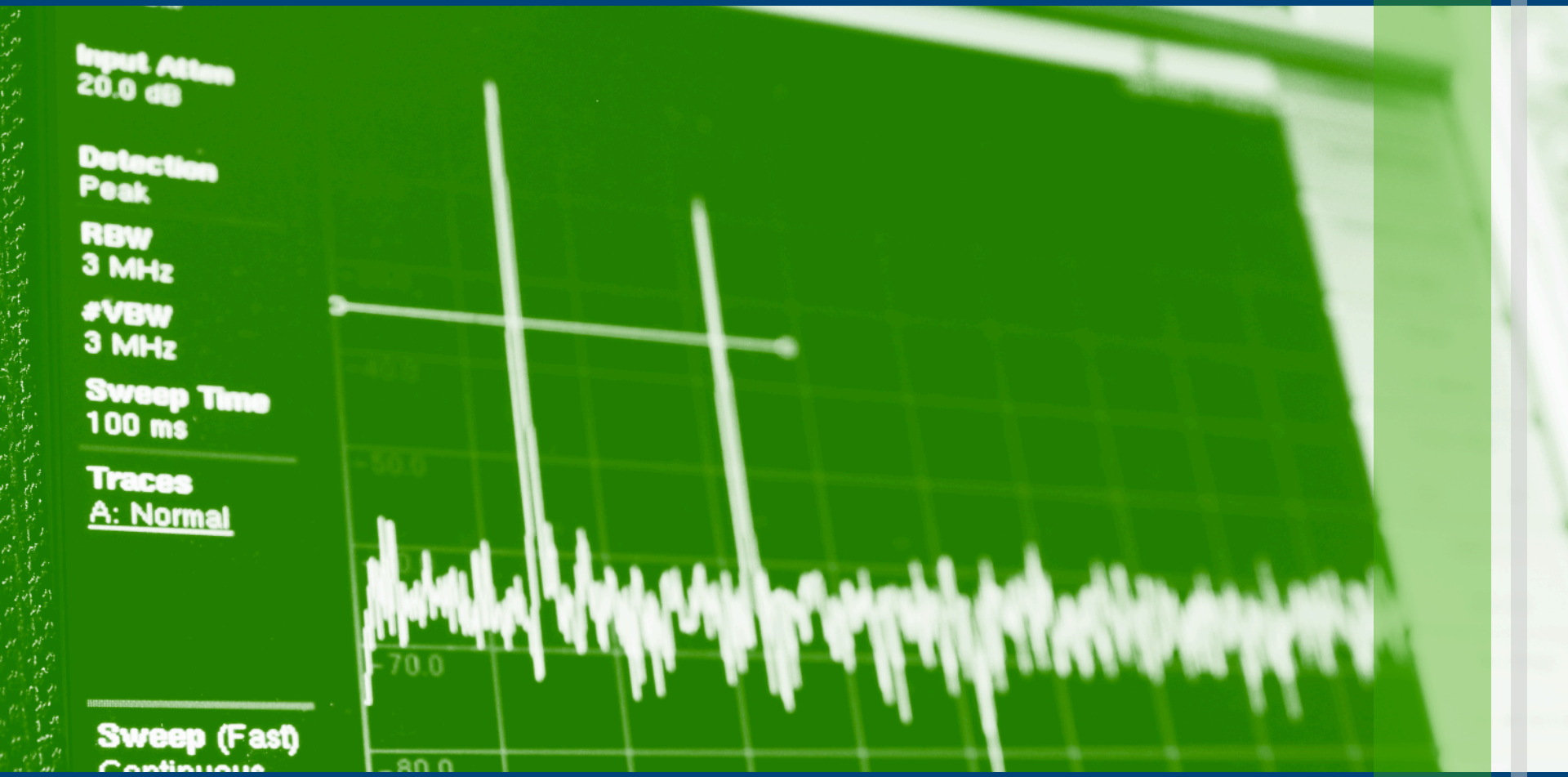
1. Share Tools to Amplify & Unify Message
2. Work with FEMA and OEC on Exercises
3. Improve Training

In order to fully implement the outcomes of JamX 17, such as training and exercise programs, in communities across the country, **it is imperative to allow time to mature and transfer the capabilities**.

DHS S&T's next First Responder Electronic Jamming Exercise will take place in 2019. JamX 19 will test how well DHS Components and the public safety community have adopted counter-jamming recommendations and will include additional interference sources and red-teaming.

How NPSTC Can Help

- FRG would like to work with NPSTC raise awareness of jamming threats and increase communications resiliency
- NPSTC members can help by:
  - Distributing knowledge products from the 2016 exercise and JamX 17, when they are ready
  - Ensuring that your organization is aware of threats and knows how to recognize, respond to, report and resolve jamming threats
  - Implementing FRG's initial recommendations and recommending that other organizations do the same
  - Encouraging reporting to the FCC



INITIAL RECOMMENDATIONS

Mitigating Jamming:
First Responder Perspective

- Communications failures are always assumed to be equipment issues
- Set operators up for success through equipment purchasing, setup and fleetmap management
- Education is key – operators must understand jamming threats to take them seriously
- Basic mitigation strategies include shielding and height

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

Reporting Jamming

- All suspected radio frequency interference **MUST** be reported to the Federal Communications Commission as soon as possible
- DHS and the FCC monitor reports of interference and jamming to conduct trend analysis and inform policy

CONTACT THE 24/7 FCC OPERATIONS CENTER

CALL
1-202-418-1122

EMAIL
FCCOPS@fcc.gov

WEBSITE
www.fcc.gov/general/public-safety-support-center

Engage With Us!

DHS S&T JAMMING EXERCISE PROGRAM

PRIMARY EMAIL
Jamming.Exercise@hq.dhs.gov

DHS S&T FIRST RESPONDERS GROUP

WEBSITE
www.FirstResponder.gov

TWITTER
@dhsscitech

EMAIL
First.Responder@dhs.gov

FACEBOOK
@FirstRespondersGroup

Homeland Security

Science and Technology