U.S. Department of Homeland Security | Science and Technology Directorate

Resilient Communications & Counter-Jamming at DHS

Science and Technology

Russell Becker
Director
Office for Interoperability & Compatibility (OIC) Technology Center
Science & Technology Directorate (S&T)

September 20, 2022

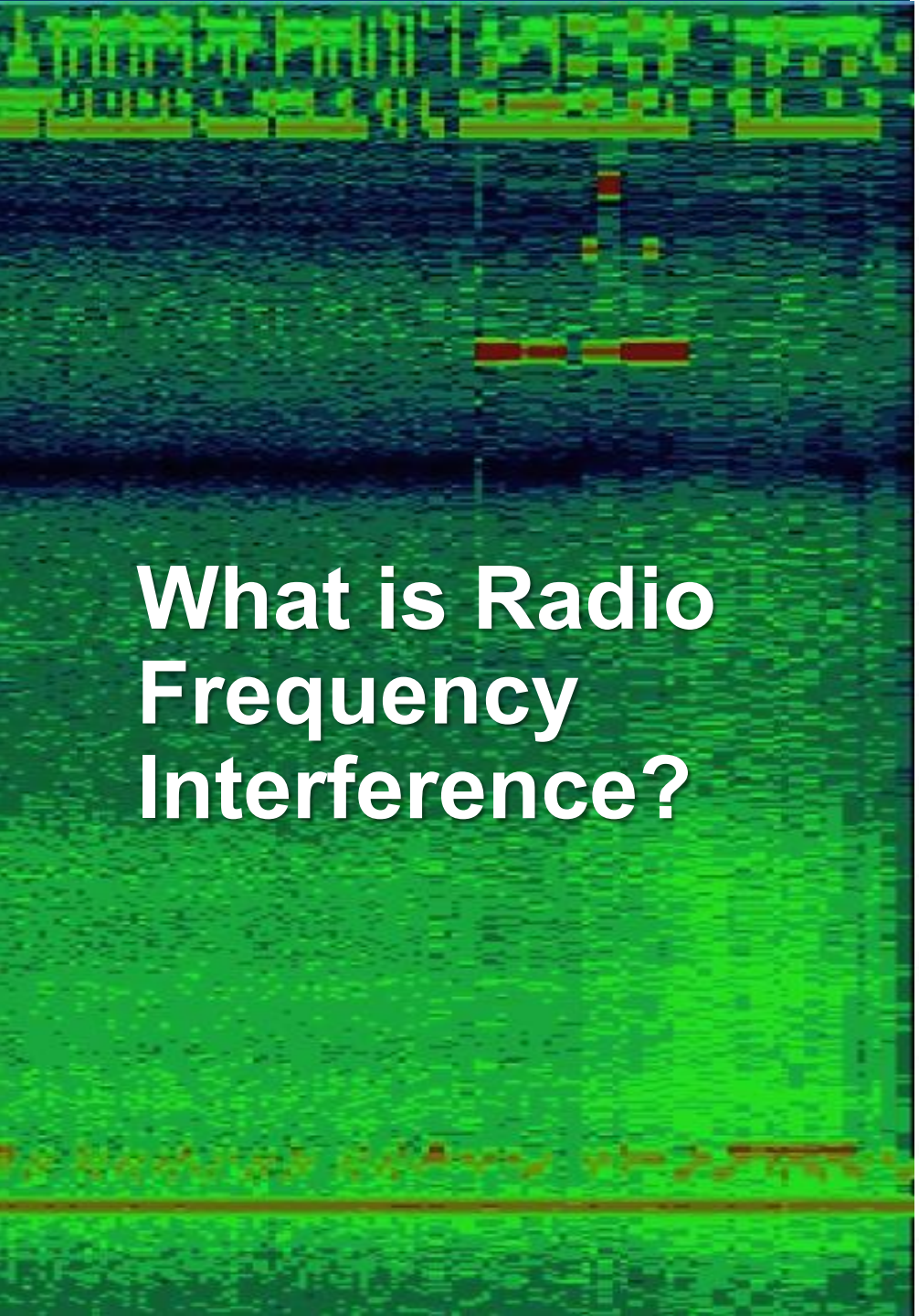
Agenda

- OIC-TC's Mission & Legislative Mandate
- Radio Frequency Interference Overview
- Jamming 101
- DHS Resilient Communications Work
  - Resilient Communications Goals
  - JamX 16
  - JamX 17
  - Resilient Communications Training
  - JamX 22
- Next Steps
- Q&A

S&T OIC-TC's Mission & Legislative Mandate

- **Mission:** Provide subject matter expertise and core research capabilities needed to ensure that S&T maintains the ability to identify and address current and future DHS component challenges in the areas of communication and network capabilities, as well as position, navigation, timing (PNT) necessary for the functioning of many critical infrastructure sectors.

- S&T OIC-TC has a legislative mandate to enable interoperability for public safety (6 USC § 195 & 195a)
  - Evaluate and assess new technology in real-world environments to achieve interoperable emergency communications capabilities
  - Understanding the strengths and weaknesses of the public safety communications systems in use
  - Evaluating and validating advanced technology concepts, and facilitating the development and deployment of interoperable emergency communication capabilities



What is Radio Frequency Interference?

Any signal that seriously degrades, blocks or repeatedly interrupts radio frequency signals

Intentional Sources

- Illegal jammers
- Unauthorized transmissions

Unintentional Sources

- Cheaply made, non-UL approved electronics and baby monitors
- Spurious emissions from malfunctioning communications equipment
- Malfunctioning signal boosters
- Poor communications planning
- Natural phenomena such as sun flares

What Does Interference Look Like?

Disruption or failure of wireless communications or mapping equipment – including cellular, Wi-Fi, Bluetooth, LMR or GPS systems – for unknown reasons could indicate interference

You may be experiencing intentional or unintentional 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"
- Experience significant static or music coming from regularly-used radio channels

Jamming 101

Jamming 101: Impacted System Examples

- Communications are a lifeline for first responders and federal law enforcement
- More than radios and phones rely on secure communications. **Jammers could impact any communications system that uses radio frequency signals (RF) –** Cellular LTE/3G/4G/5G/6G, GPS, Land Mobile Radio, Wi-Fi, Bluetooth
- **Virtually all systems reliant on RF signals are vulnerable to jammers**, including:
  - 9-1-1 and dispatch calls
  - Command and control systems
  - Hazmat detectors
  - Wireless sensor networks
  - Fire department mayday transmissions
  - Alarm and security systems
  - Alerts and warnings
  - Location services
  - Undercover surveillance
  - K-9 law enforcement response
  - Remote control robots (e.g., bomb squad robots)
  - Unmanned Aircraft Systems units
  - On-body or environmental sensors
  - Video and photo transmission

What is Jamming?

- Jamming is a **denial-of-service attack** that can target any communications system that uses radio frequency signals (RF)
- Jammers emit RF signals at specific bands to overpower and block other signals, such as authorized communications transmissions
  - A communication system is “jammed” when the noise has significantly degraded or blocked the receiver's ability to correctly process the desired signal
- Jammers are often cheaply manufactured overseas and are low-quality electronics, which means that they often emit inconsistent signals, making them hard to detect

Jammer Varieties

- Jammers come in all shapes and sizes, and are often disguised to look like something else, such as a USB flash drive, box of cigarettes, or Wi-Fi router
  - Some varieties do not even have visible antennas
  - Systems can be co-opted to conduct jamming (e.g., stolen radios, radios bought commercially)
- Jammers can be custom ordered to target specific bands or frequencies
- There are Do-It-Yourself tutorials on YouTube on how to build jammers

Jamming Legal Review

- Manufacturing, importing, marketing, selling or operating of jamming devices is ILLEGAL in the United States (47 U.S.C. § 302a(B))
  - This law **does not prohibit owning, buying, or exporting jammers**
  - DHS S&T and CISA are working with FCC to close this loophole
- 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)
- State and local law enforcement actions against jammers are not authorized under these laws, as only the FCC Enforcement Bureau has jurisdiction
  - Some states and municipalities have established laws or regulations to address this gap
- All Federal, State, Local, Tribal, and Territorial agencies should talk with their legal counsel about legal authorities available to their agency, including any applicable state or municipal regulations
  - As appropriate, jamming incidents may be prosecuted as interfering with police business or as a cybercrime, in addition to jamming-specific charges

DHS Resilient Communications Work

DHS Goals for Resilient Communications

1. **Improve communications resiliency** to jamming and other interference threats by increasing 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

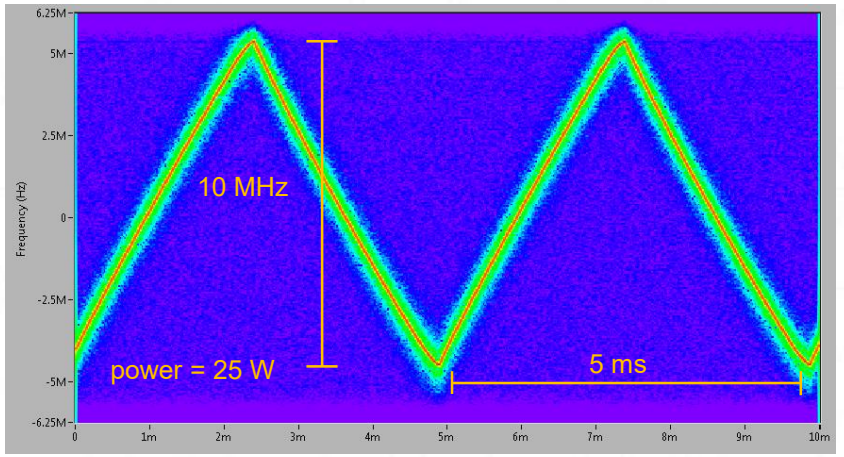
COTS Jammers

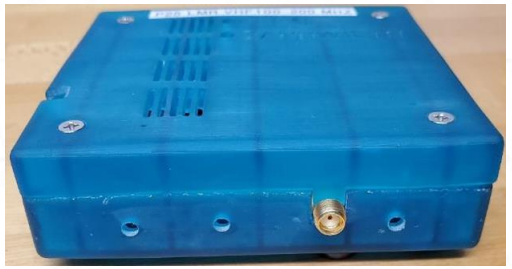
- S&T worked with ICE Homeland Security Investigations out of New Jersey in 2015-2016 to purchase illegal jammers as part of a law enforcement investigation
- This assortment of low-cost, Chinese-made jammers available for purchase on internet
  - Representative of threat that an unsophisticated adversary might deploy
- By JamX 17, the performance of the jammers had significantly degraded
- As the devices were no longer reliable for testing, S&T decided to build new jammers based on commercial specs that would more reliably perform for testing consistency

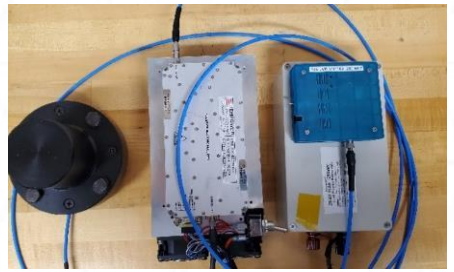
S&T-Developed Jammers

- S&T's custom-built jammers were designed to COTS specs, ensuring they are representative of likely threats
- Multiple RF outputs per unit covering a variety of fixed frequency bands
- Continuous linear frequency modulation (LFM)
  - "Sawtooth" or "triangle" LFM pattern
  - Typical period of several microseconds to 10's of microseconds (At least one unit has period of 600 microseconds)
  - Span of 10's of MHz to 100+ MHz per band
- Up to 15W per channel
  - Typical Power Spectral Density (PSD) of 10 to 25 dBm/MHz

Typical Spectrogram







Science and Technology

Resilient Communications Training

- DHS wants to make mission-critical communications (federal, state, local) more resilient to all communications denial, interruptions, and threats, not only jamming
- To achieve this vision, CISA Emergency Communications Division developed **Resilient Communications Training** based on JamX 16 and JamX 17 results to **prepare mission-critical operational and technical personnel to mitigate and overcome communications interruptions to achieve the mission objective**
- Two Courses:
  - **Resilient Communications Awareness** – 2.5-hour instructor lead virtual course that provides first responders with basic radio frequency (RF) characteristics and enable tactics to recognize, overcome, and report loss of communications
  - **Resilient Incident Communications Management** – 8-hour in-person course that provides trained Communications Unit and public safety agency communications technical personnel with enhanced communications resiliency planning and RF interference recognition capabilities, enabling better preparedness and rapid mitigation of communications obstacles

Resilient Communications Awareness Course

Basics of Interference

The Awareness Course taught us that…

- Pine trees cause problems,
- Jamming is rare
- Try Statue of Liberty,
- PACE it from there.

Strategies and Tactics for Restoring Comms

Move through COMMS on your Primary options then Alternate, Contingent, and Emergency.

Science and Technology

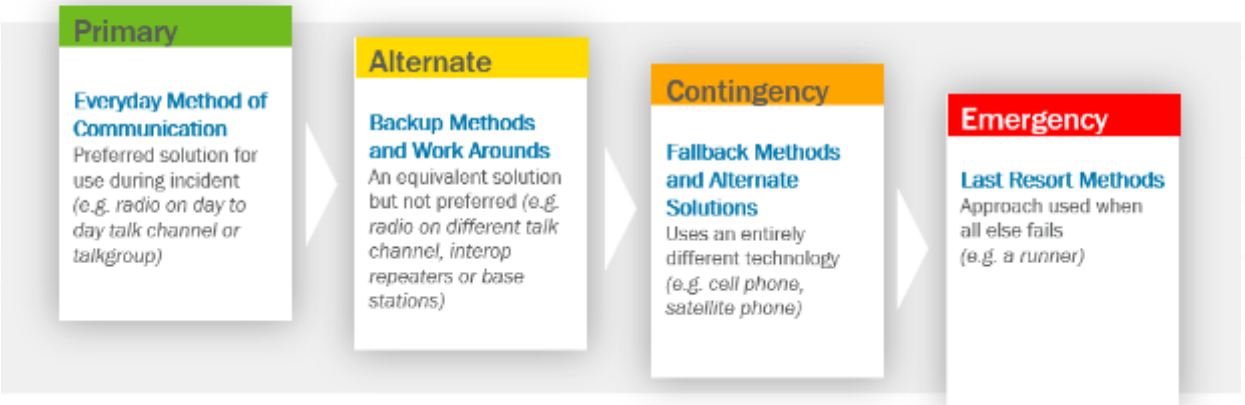
Resilient Incident Communications Management Course

Radio Frequency (RF) Interference Mitigation Lifecycle

Building blocks that lead to resilient communications

Follow your PACE Plan

The PACE plan is expressed as a list in order of communication precedence.



Science and Technology

JamX 22 Goals

Operation Trinity

Assess the effectiveness of the Resilient Communications Training for operational and technical personnel

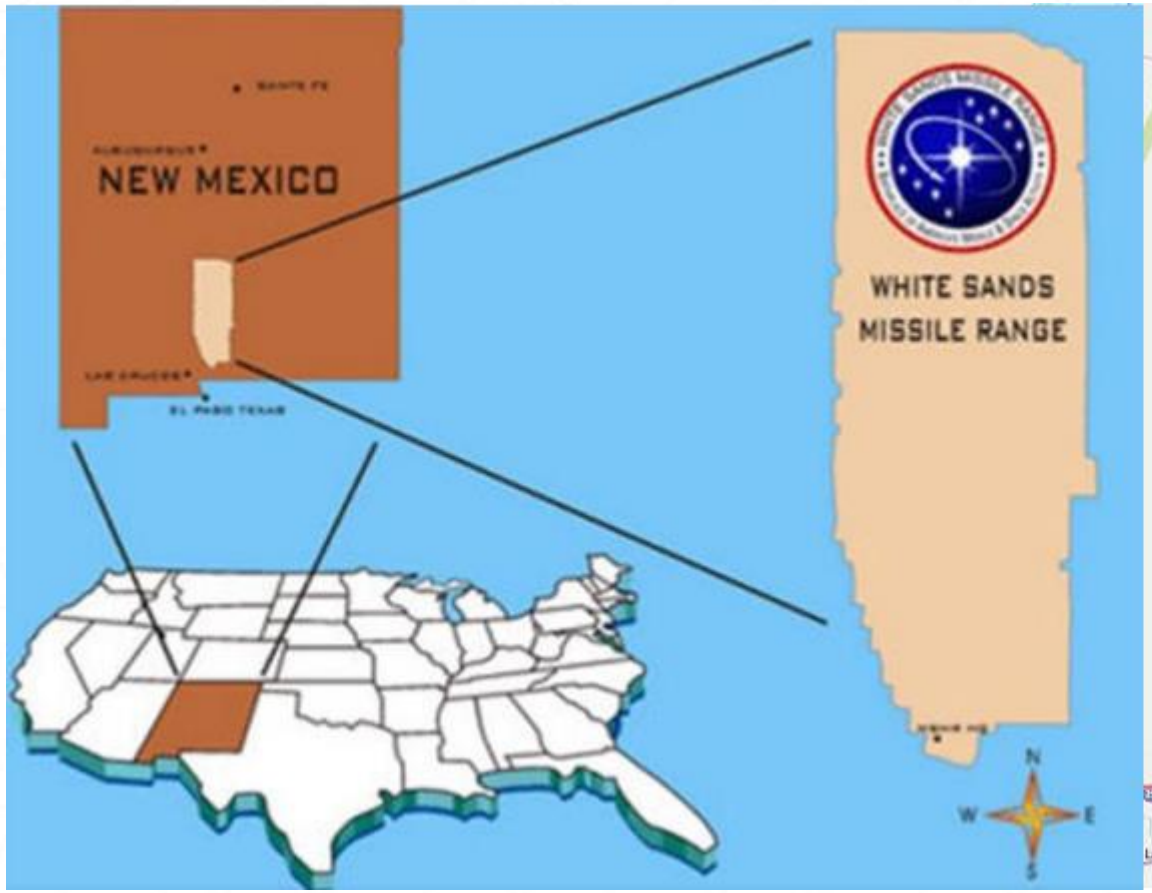
- Evaluate responder and federal operational and technical personnel in response scenarios with jamming to assess how effective the training is at enabling users to complete the mission and reestablish communications
- Validate the training and identify any needed improvements prior to nationwide deployment

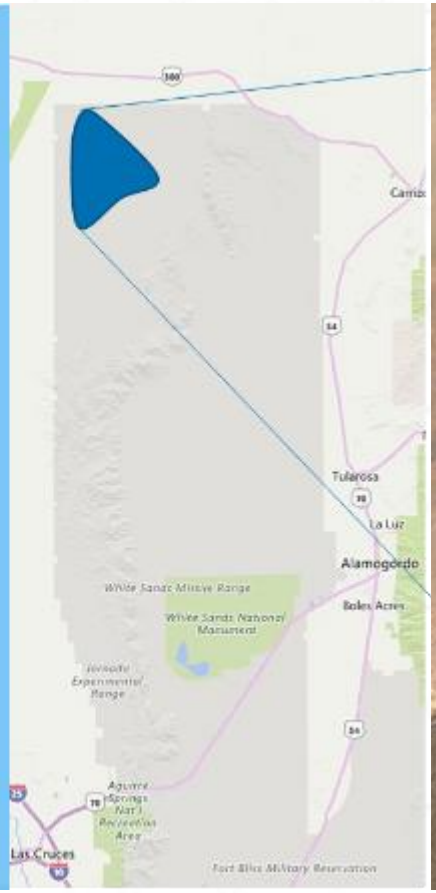
Project Resilience

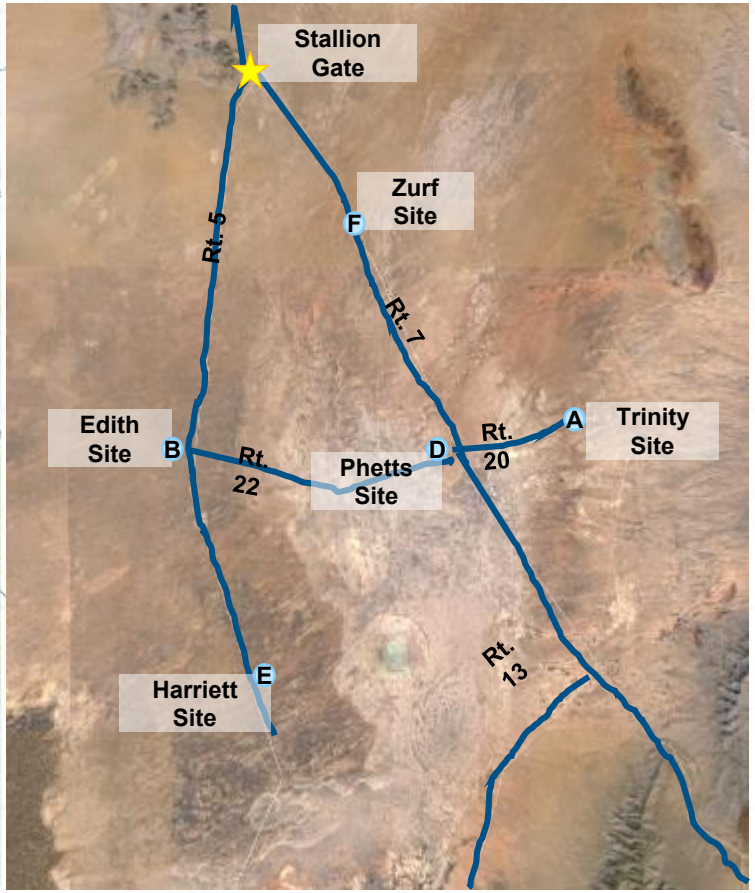
Assess tools and technologies to identify, locate, and mitigate spectrum interference

- DHS developed tools (MISCAN)
- Commercial technologies (from industry partners on CRADAs)
- Carriers and communications providers

Venue: White Sands Missile Range







Science and Technology

JAM X 22

BY THE NUMBERS

- §~220 attendees
  - §62 player participants
    - §12 STL agencies from 11 states
    - §4 DHS Components & 3 HQ offices
  - §63 vendor participants
    - §15 companies
  - §96 CISA, S&T, and partner staff
  - §26 VIPs
- §12 custom-built jammers
- §6 WSMR Test Sites over 800 sq mi of desert
- §3 S&T-funded solutions
- §2 CISA-funded training courses

Operation Trinity Overview

- **Approach**: Develop and evaluate mission-critical resilient communications training
  - **Resilient Communications Awareness** – 2.5-hour instructor lead virtual course that provides first responders with basic RF characteristics and enable tactics to recognize, overcome, and report loss of communications
  - **Resilient Incident Communications Management** - 8-hour in-person course that provides trained Communications Unit and public safety agency communications technical personnel with enhanced communications resiliency planning and RF interference recognition capabilities, enabling better preparedness and rapid mitigation of communications obstacles
- **Outcomes**: Evaluated training through targeted scenario exercise stations and conducting real-time adversarial team competition

Operation Trinity Participants

Training Evaluation Staff

ECD – Interoperable Communications Technical Assistance Program
ECD – National Governance
ECD – Priority Telecommunications Service
IOD – Emergency Response Operations
IOD – Regions 3, 8, and 9

Naval Information Warfare Center PACIFIC

Science and Technology

FEMA

NC DIT

Operational Players

DPS

KOEC

PIMA COUNTY

NM

Project Resilience Overview

- **Test Objectives**
  - Identify the threat factor/susceptibility/vulnerability of jammers on communication systems
  - Evaluate the effective use of mitigation and counter-measure to identify, locate and mitigate jamming
  - Identify any Research & Development (R&D) gaps
  - Give vendors an opportunity to test their technologies in a structured over the air jamming environment
  - Evaluate S&T-developed technologies
- **General Test Scenarios (Examples)**
  - Quantify impact of various jammers / waveforms on 4G/5G downlink
  - Quantify impact of various jammers / waveforms on 4G/5G uplink
  - Quantify impact of various jammers / waveforms on LMR portable radio
  - Quantify impact of various jammers / waveforms on LMR base station
- **Jammer Variables**
  - Jammers provided by DHS S&T: COTS, JVAB
  - Jammers provided by Project Resilience participants: CACI, LinQuest/TMC Design, Motorola, SOC-USA, and Syncopated

Project Resilience Participants

Victim Comms Infrastructure

Motorola
- LMR base station and radios

OUSD
- T-Mobile 4G/5G COLT

Sandia / DARPA
- OPS-5G System

CACI
- NetGo 4G LTE

Interference Sources

TMC Design
- Portable Jamming System (PJS)

Syncopated
- Mockingbird

CACI
- Chameleon
- Gecko

Motorola
- SUPPRESS

SOC
- Cameleon arbitrary signal generator and transmitter

DHS S&T
- COTS jammers
- JVAB jammers

Identification / Location / Mitigation Technologies (Commercial Ready-to-Deploy Systems)

Rohde & Schwarz
- MobileLocator system

PCTEL
- SeeHawk Monitor
- SeeWave

SOC
- Fixed Monitoring Unit (FMU)
- Portable Monitoring Unit (PMU)
- LS OBSERVER

Anritsu
- Field Master Pro (MS2090A)
- Remote Spectrum Monitor (MS27102A)

CACI
- Spectral Vision System
- Spectrum Guard
- NetGo 4G

Identification / Location / Mitigation Technologies (Prototype / Development Systems)

Motorola
- MSI Overwatch

Epiq Solutions
- PRiSM sensor

Syncopated
- CIELO

DHS S&T
- MISCAN

Next Steps

JamX 24

- Evaluate jamming of data networks (5G/6G) and devices (IoT, robots, unmanned systems, etc.)
- Expand Resilient Communications Training to cover LTE, data, and video interference
- Evaluate expanded Resilient Communications Training with first responders