2017 First Responder Electronic Jamming Exercise

Homeland Security
Science and Technology

THE JAMMING THREAT

Jamming communications systems—including GPS, radio, cellular and wireless systems—poses a threat to law enforcement and public safety across the country. Illegal jammers could interfere with public safety communications and may leave responders without access to backup. Proliferation of jamming devices may delay emergency response times, escalate hazardous situations, facilitate illicit activities, or result in loss of life.

The DHS Science and Technology Directorate (S&T) is resolute in making first responders safer and more aware of jamming and its potential impact to their communications, safety, and ability to execute their mission. S&T is combatting jamming threats by evaluating the threat, developing and testing mitigation technologies, working with public safety agencies to update training procedures, and raising awareness of jamming threats and characteristics.

ACCOMPLISHMENTS TO DATE

As a first step, S&T hosted the 2016 First Responder Electronic Jamming Exercise, a multi-agency operational exercise at White Sands Missile Range, in New Mexico. The exercise also sought to demonstrate how jamming affects federal and public safety communications systems and how responders can recognize and react to jamming.

Building on the findings from 2016, DHS S&T hosted the 2017 First Responder Electronic Jamming Exercise at the U.S. Department of Energy's Idaho National Laboratory in July 2017. During the event, S&T assessed the effectiveness of jamming identification, localization and mitigation technologies and tactics.

IDENTIFY, LOCATE AND MITIGATE JAMMING

S&T invited federal, state, local and tribal law enforcement and public safety organizations, as well as representatives from academia and industry, to participate in the event. Participating tactical and observational teams gained valuable exposure to jamming environments in a controlled and approved test

environment, which better prepared them to face real-world jamming incidents, develop solutions and help make our nation more resilient to jamming attacks. S&T and other participants authenticated how identification, location and mitigation technologies and tactics increased communications resiliency against jamming threats.

Based on the 2017 results, S&T and partners are working to develop comprehensive recommendations for federal, state and local law enforcement and public safety organizations to help them recognize, respond to, report and resolve jamming incidents. S&T's goal is that every first responder be aware of and prepared for jamming threats. Following the exercise, S&T:

- Awarded three Phase I and one Phase II Small Business Innovation Research Grants to develop low-cost sensors to detect jamming interference and alert responders to the hazard;
- Added two new topics to FEMA's Authorized Equipment List to help agencies purchase tools via grant funding that will enable them to better identify and locate interference: 06CP-07-RFDF - Equipment, RF Direction Finding and 06CP-07-RFSA - Equipment, RF Detection and Spectrum Analysis; and
- Coordinated with the DHS Cybersecurity and Infrastructure Security Agency, SAFECOM, and the National Council of Statewide Interoperability Coordinators to develop a Public Safety Radio Frequency Interference Best Practices Guidebook.