



Emergency Management and Response Information Sharing and Analysis Center (EMR-ISAC)

INFOGRAM 46-10

November 18, 2010

***NOTE:** This INFOGRAM will be distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures. For further information, contact the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at emr-isac@dhs.gov.*

Radio Frequency Jamming

(Source: National Coordinating Center for Telecommunications)

At the request of the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC), the [Communications—Information Sharing and Analysis Center](#) provided current information regarding radio frequency jamming incidents and the risks to public safety communications.

The following facts from a Communications ISAC presentation are summarized below for the awareness of Emergency Services Sector departments and agencies:

- Radio frequency jammers are designed to transmit radio signals to disrupt or prevent legitimate, authorized radio communications over certain frequencies.
- Jamming incidents affecting wireless or cellular services and Global Positioning Services (GPS) are increasing in the U.S. and abroad.
- Jammers may be very small, low-power devices that fit in a shirt pocket or a much larger unit almost the size of a microwave oven.
- The effective range of jammers extends from about five meters radius to several kilometers.
- The Communications Act of 1934 strictly prohibits the use of jammers.
- A Public Notice issued by the Federal Communications Commission (27 June 2005) reinforced that the sale and use of jammers in the U.S. is prohibited.
- The operation of jammers could severely undermine critical public safety communications, e.g., E-911, priority access services, emergency alerts, aviation control systems, etc.
- The Association of Public-Safety Communications Officials (APCO) and the National Emergency Number Association (NENA) have opposed jammers due to their impairment of emergency communications and commercial wireless networks.

Maintaining Operational Capabilities during a Pandemic

(Source: Department of Homeland Security)

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) recently received the "[Information for First Responders on Maintaining Operational Capabilities during a Pandemic](#)" (PDF, 633 KB) from the Department of Homeland Security (DHS) Office of Health Affairs (OHA). It is the result of a joint effort by the DHS OHA and U.S. Fire Administration with major contributions from a working group of first responders.

The document intends to support endeavors by emergency responders to provide the best possible service to their team and community, while contributing to a safer and healthier responder workforce. It particularly provides the following kinds of information for first responders:

- Potential ways to adjust operations to maintain readiness and response.
- Two planning tools for leaders in the emergency responder community at the local level.
- Reference sheets with discipline-specific possible action steps.

According to the Executive Summary, in the midst of a pandemic, the leaders and operators of the emergency services should integrate this information with their existing planning efforts, knowledge, experience, and training, and apply it to their specific situation when appropriate. “Better-protected first responders can better protect their communities.”

Intelligence-Led Mitigation

(Source: Journal of Homeland Security and Emergency Management)

The 2010 issue of the [Journal of Homeland Security and Emergency Management](#) contains the article titled “[Intelligence-Led Mitigation](#).” The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) noted that the paper explores methods for capitalizing on existing law enforcement intelligence capabilities to provide intelligence support to decision makers for a full spectrum of public safety and emergency services operations.

The Abstract for this paper explains that intelligence-led mitigation is a management philosophy and business process to proactively guide strategic, operational, and tactical decisions for mitigating the effects of intentional, accidental, and natural incidents. “The premise of intelligence-led mitigation includes the intelligence-led policing approach for systematically collecting, organizing, analyzing, and utilizing intelligence to make informed resource decisions.

Within this document, the EMR-ISAC further observed that the intelligence-led mitigation model was designed to demonstrate how the existing principles and processes of intelligence-led policing can be applied to a broader set of incidents, incident phases, and stakeholders in order to effectively fill this critical intelligence gap. “The goal of intelligence-led mitigation is to provide organizations with public safety and emergency services functions (e.g., police, fire, EMS) with intelligence products which enhance their understanding of the operational environment and enable them to make informed resource decisions on appropriate preparedness, prevention, protection, response, and recovery actions to mitigate incidents.”

Emergency Communications Forum

(Source: DHS, Office of Emergency Communications)

The Department of Homeland Security (DHS) [Office of Emergency Communications](#) (OEC) notified the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) regarding the release of Volume IV of the [Emergency Communications Forum \(ECF\) newsletter](#) (PDF, 3 MB). The ECF engages and informs emergency responders; policy makers; and federal, state, local, and tribal officials about issues and events that directly affect everyday nationwide emergency communications.

Volume IV of the ECF newsletter highlights California emergency response agencies that recently completed [National Emergency Communications Plan Goal 1](#) as well as interoperability efforts in Texas. This edition also delves into partnerships between the U.S. and Canada’s interoperability programs, and provides updates on OEC’s [Regional Coordination](#) program.

The OEC invites interested personnel to subscribe to the ECF newsletter by sending e-mail to OEC@hq.dhs.gov. Those who wish to submit an article pertaining to emergency communications in the field, best practices, and lessons learned can send their information to the same electronic address.

Note: There will be no INFOGRAM published on Thanksgiving Day, Thursday, 25 November 2010.

DISCLAIMER OF ENDORSEMENT

The U.S. Fire Administration/EMR-ISAC does not endorse the organizations sponsoring linked web sites, and does not endorse the views they express or the products/services they offer.

FAIR USE NOTICE

This INFOGRAM may contain copyrighted material that was not specifically authorized by the copyright owner. EMR-ISAC personnel believe this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

REPORTING NOTICE

The National Infrastructure Coordinating Center (NICC) within the Department of Homeland Security (DHS) Office of Infrastructure Protection is the central point for notifications regarding infrastructure threats, disruptions, intrusions, and suspicious activities. Emergency Services Sector personnel are requested to report any incidents or attacks involving their infrastructures using at least the first and second points of contact seen below:

- 1) NICC - Voice: 202-282-9201, Fax: 703-487-3570, E-Mail: nicc@dhs.gov
- 2) Your local FBI office - Web: www.fbi.gov/contact/fo/fo.htm
- 3) EMR-ISAC - Voice: 301-447-1325, E-Mail: emr-isac@dhs.gov, fax: 301-447- 1034,
Web: www.usfa.dhs.gov/emr-isac, Mail: E-108, 16825 South Seton Avenue, Emmitsburg, MD 21727