



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

INFOGRAM 36-11

September 8, 2011

***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.*

Tenth Anniversary of the 9/11 Attacks

(Source: DHS)

For ten years this nation has enjoyed the absence of a major terrorist attack. Much credit for this belongs to the combined efforts of many public and private entities that altered their plans, training, and operations to prevent and protect against the next man-made catastrophe. Despite severely restrained resources, these organizations avoided complacency and mediocrity by improving their capabilities to deter or mitigate the cataclysmic effects from all hazards. The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) applauds the smart and hard infrastructure protection and resilience work ongoing throughout America, particularly by emergency responders.

In a recent [statement](#), Secretary of Homeland Security Janet Napolitano explained that there is no specific or credible intelligence that al-Qaida or its affiliates are plotting attacks in the United States to coincide with the ten-year anniversary of 9/11. However, she stated: “We remain at a heightened state of vigilance and security measures are in place to detect and prevent plots against the United States should they emerge.”

Secretary Napolitano elaborated that Homeland Security is a shared responsibility and everyone plays an important role in helping to keep communities safe and secure. “We remind our federal, state, local partners, and the public to remain vigilant and to report any suspicious activity to local law enforcement authorities.”

Public Health Preparedness Guidance

(Source: CDC)

Because of its unique abilities to respond to infectious, occupational, or environmental incidents, the Centers for Disease Control and Prevention (CDC) plays a pivotal role in ensuring that state and local public health systems are prepared for these and other public health incidents. To assist state and local health departments with their strategic planning, the CDC implemented a systematic process for defining a set of public health preparedness capabilities.

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) confirmed that the CDC released “[Public Health Preparedness Capabilities: National Standards for State and Local Planning](#)” (PDF, 2.9 Mb) to provide guidance in identifying preparedness gaps, accelerating planning, determining specific jurisdictional priorities, and developing plans for building and sustaining capabilities. These standards are designed to accelerate state and local preparedness planning, provide guidance and recommendations for preparedness planning, and to assure safer, more resilient, and better prepared communities.

The Public Health Preparedness Guidance covers six categories and identifies 15 public health preparedness capabilities, including emergency operations coordination, fatality management, mass care, medical surge, public health biosurveillance, epidemiological investigation, and responder safety and health. The 15 capability sections in this document are intended to serve as national standards that state and local public health departments can use to advance their preparedness planning.

Chemical Suicides Training Program

(Source: Fire Engineering)

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) learned that the [Firefighters Support Foundation](#) has a new training program titled “[Chemical Suicides](#),” which is now available free by download. This program can be obtained in two formats: a 36-slide PowerPoint program, and a 23-minute video program.

First responders can view the video material with the PowerPoint file acting as their hard copy notes. Alternatively, they can use either resource independently. The program intends to accomplish the following:

- Explain the process of chemical suicide by mixing cheap and easily available chemicals in an enclosed space.
- Describe why it is a popular way of committing suicide and a growing threat to responders.
- Define the reasons why responders may be exposed to the lethal gases produced by the process.
- Educate responders about the warning signs that they may be approaching a chemical suicide.
- Suggest response tactics and guidelines.

More information about this phenomenon can be seen at the [Homeland Security Newswire](#).

“Anonymous” Operations

(Source: eWeek.com)

The loosely organized hacking collective known as “Anonymous” announced through several mediums that they plan to conduct cyber attacks, peaceful protests, and other unspecified activity targeting a variety of organizations, according to an unclassified [bulletin](#) by the [National Cybersecurity and Communications Integration Center](#) (NCCIC).

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) noted that “[Anonymous](#)” recently struck the websites of the Arizona Department of Public Safety and the Arizona chapter of the Fraternal Order of Police, temporarily bringing both domains offline. It continues to devote resources to creating new cyber attack and exploitation tools. According to this hacking group, they are working on a new attack tool called “#RefRef” that is able to use a server’s resources and/or processing power to conduct a denial of service against itself.

Throughout the past decade, several racist, homophobic, hateful, and otherwise maliciously intolerant cyber and physical incidents have been attributed to “Anonymous.” More recently, their targets and apparent motivations have evolved to what appears to be an agenda driven by social, religious, political or cultural ideology.

More information regarding the operations of “Anonymous” can be seen at this NCCIC [bulletin](#) (PDF, 482 Kb). Technical assistance to protect Emergency Services Sector departments and agencies from “Anonymous” operations can be obtained from the [United States Computer Emergency Readiness Team](#) (US-CERT).

DISCLAIMER OF ENDORSEMENT

The EMR-ISAC does not endorse the organizations sponsoring linked websites, 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

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI office and also the State or Major Urban Area Fusion Center. FBI phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm>. Fusion Center information can be seen at <http://www.dhs.gov/contact-fusion-centers>.

For information specifically affecting the *private sector* critical infrastructure contact the National Infrastructure Coordinating Center by phone at 202-282-9201, or by email at nicc@dhs.gov.

When available, each report submitted should include the date, time, location, type of activity, number of people, equipment used for the activity, name of submitting person and organization, and a designated point of contact.