



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

INFOGRAM 15-09

April 16, 2009

***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.*

OPSEC Review

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) recently learned of an Emergency Services Sector (ESS) organization that posted its policies for handling different kinds of emergency scenarios on the city's web site for public access. According to local media, "some of the rules are mundane, but others reveal the inner workings of the department that could put their lives at risk if the wrong people should learn about them."

Emergency departments and agencies have an abundance of critical information of high value to adversary intelligence collectors as well as local criminals. Therefore, it is crucial for ESS leaders, owners, and operators to evaluate their operations from the viewpoint of domestic and transnational actors who intend to harm personnel or degrade operations. For example, EMR-ISAC research substantiates that criminal and terrorist elements desire sensitive information regarding capabilities for various emergencies, command structure, incident command protocols, levels of competence, apparatus and equipment status, mutual aid agreements, emergency plans, standing operating procedures, response times, preferred routes, radio frequencies, call signs, key structure floor plans, etc.

It is important to note that open source information yields much of the intelligence terrorists apply to plan attacks. Posting documents for public access containing any of this information can potentially provide nefarious individuals with insights to assist their planning against an organization's survivability, continuity, and response-ability. Hence, ensuring that sensitive information is not shared with the public is an essential part of Operations Security (OPSEC). OPSEC is an analytical process to identify, control, and protect sensitive, but unclassified information for the purpose of denying opponents data they can synthesize to compromise an organization's operations, safety, and security.

The Interagency OPSEC Support Staff (IOSS) was created to support the National OPSEC Program by providing tailored training, assisting in program development, producing multimedia products, and presenting conferences for the defense, security, intelligence, research and development, acquisition, and public safety communities. Its mission is to help organizations develop their own, self-sufficient OPSEC programs to protect critical infrastructures and key resources. Some of the IOSS programs are designed specifically for ESS departments and agencies.

For more information about OPSEC training and programs, contact the IOSS at 443-479-4677 or at ioss@radium.ncsc.mil.

Social Networking Security Risks

The popularity of social networking sites, such as MySpace, Facebook, Twitter, and others, has exploded in recent years. Because these sites are equally popular with adults, according to the Pew Internet & American Life Project, they can be found on many official work stations in addition to home personal computers. While there are positive aspects of using social networking sites, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) confirmed the necessity to understand the potential security risks and the precautions to take to protect yourself and your organization.

Social networking sites are online communities of Internet users who want to communicate with other users about areas of mutual interest, whether from a personal, business, or academic perspective. Although the specific functionality of the various sites may differ, they generally allow you to provide information about yourself and correspond with others through e-mail, chat rooms, and other forums.

With the assistance of the National Cyber Security Division and Multi-State ISAC, the EMR-ISAC verified that social networking sites are growing in popularity as attack vectors because of the volume of users and the amount of information that is posted. Considering the perceived anonymity and false sense of security of the Internet, users occasionally provide more information about themselves and work-related issues than they would to a stranger in person. Therefore, Emergency Services Sector (ESS) personnel should comprehend that information posted online could be used to conduct social engineering scams intended to steal sensitive organizational or personal identity information. Additionally, these sites are increasingly the sources of worms, viruses, and other malicious code.

The Multi-State ISAC recommends the following actions to protect yourself (and your department or agency if using a work computer) before visiting a social networking site:

- Ensure the computer has a firewall, updated anti-virus software, and current operating system.
- Do not assume you are in a trusted environment when on someone's web page.
- Exercise common sense and caution when communicating with someone you do or do not know.
- Limit how much personal or professional information you provide to anyone.
- Pay close attention to the policies and terms of the sites to ascertain if they are sharing your information.
- Never forget that posted information can be viewed by a broad audience and could have lasting implications.

For more information regarding the security risks of social networking sites, see the National Cyber Alert System Cyber Security Tip at <http://www.us-cert.gov/cas/tips/ST06-003.html>.

Revised CBRN PPE Standards

The National Institute for Occupational Safety and Health (NIOSH) released "Recommendations for the Selection and Use of Respirators and Protective Clothing for Protection Against Biological Agents," designed to protect Emergency Services Sector (ESS) responders in the aftermath of a biological weapons attack.

NIOSH Associate Director for emergency preparedness, John Decker, explained that when the previous guidelines were published in 2001, there was no breathing gear that offered protection against all four types of hazardous agents: chemical, biological, radiological, and nuclear (CBRN). The new guidelines, released last week, include breathing apparatus assessed to protect against CBRN materials, and cite revised National Fire Protection Association protective clothing standards.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) noted the following highlights from the revised Personal Protective Equipment (PPE) recommendations:

- Emergency responders should use combination respirators and the highest-protection suits available when the nature of an airborne agent or its method of release is uncertain. Fewer precautions are necessary when the type of substance has been ascertained and the material is found in "a letter or package that can easily be bagged."
- The standards, specifically "oriented toward acts of terrorism," address other types of breathing gear, equipment decontamination techniques, precautionary vaccine regimens, and medical treatments and checkups that would follow exposure to a dangerous material.
- Circumstances in which non-CBRN respirators can be used, and decontamination of protective equipment after use, are discussed.

The guidelines are available at <http://www.cdc.gov/niosh/docs/2009-132/>.

AFG and JAG Application Periods Open

The application period for the Department of Homeland Security (DHS) FY2009 Assistance to Firefighters Grants (AFG) Program opened 15 April and closes on 20 May 2009, at 5:00 p.m. Eastern Daylight Time (EDT). The AFG awards, distributed nationally in phases, will ultimately provide approximately \$510 million to fire departments and nonaffiliated emergency medical services (EMS) organizations. AFG awards are intended to enhance response capabilities and enable Emergency Services Sector (ESS) organizations to purchase or receive training, conduct health and safety programs, and buy equipment and response vehicles.

An online tutorial that walks applicants through the preparation and submittal of competitive applications, and provides an overview of the funding priorities and evaluation criteria, is available at www.firegrantsupport.com/afg. Applicants also can call the AFG help desk at 1-866-274-0960. During the application period, the help desk will operate Monday through Friday, from 8:00 a.m. to 8:00 p.m. (EDT), but is prepared to revise hours of operation based on volume and demand.

The National Volunteer Fire Council (NVFC) is offering an online AFG grant narrative resource center to help volunteer fire departments write grant application narratives. Copies of narratives from successful past grant applications that can be used for example or reference purposes only (i.e., not to be copied directly) are available at www.nvfc.org/news/2007-afg-safer.html.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) also examined funding opportunities for law enforcement agencies. The Department of Justice, Office of Justice Programs, Bureau of Justice Assistance is accepting applications for more than \$4 billion in funding available under the Recovery Act: Edward Byrne Memorial Justice Assistance Grant (JAG) Formula Program. Applications for grants (including support for hiring) to assist state, local, and tribal law enforcement agencies are due no later than 8:00 p.m. EDT on 18 May 2009.

The EMR-ISAC noted that JAG Program funds can be used for a variety of efforts such as hiring law enforcement officers, supporting drug and gang task forces, funding crime prevention and domestic violence programs, and supporting courts, corrections, treatment, and justice information-sharing initiatives. Included in a list of how some jurisdictions will use the funds is a police department that will create new positions, including a "Volunteers in Police Service" coordinator. The new civilian position will free up sworn law enforcement officers to return to regular duties, and expand efforts to use volunteers to provide a wide array of services to the community. (<http://www.policevolunteers.org>)

The procedure for allocating JAG grants is based on a formula of population and violent crime statistics, in combination with a minimum allocation to ensure that each state and territory receives an appropriate share of funding. The 2009 JAG grant application package can be accessed at <http://www.ojp.usdoj.gov/BJA/recoveryJAG/JAGrecoveryLocal.pdf>.

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: <http://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/subjects/emr-isac, Mail: J-247, 16825 South Seton Avenue,
Emmitsburg, MD 21727