



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

INFOGRAM 39-08

October 9, 2008

***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.*

ESS Multi-Agency Response a Success

A U.S. Fire Administration (USFA) technical report released this week found that the Apex (North Carolina) Fire Department's (AFD) response to a chemical fire in 2006 was virtually a textbook application of Unified Command and the National Incident Management System (NIMS). According to U.S. Fire Administrator Greg Cade, "Once again we see the positive outcomes of preplanning, practicing the plans, and executing the plans when an emergency occurs."

"Chemical Fire in Apex, North Carolina" describes how the AFD led the response to the chemical fire and toxic plume, while continuously reacting to dangerous and changing conditions and successfully evacuating 17,000 citizens. There were no fatalities. Thirty civilians and 13 members of the Emergency Services Sector (ESS) were treated for respiratory distress.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-SAC) learned from the report that the Apex Fire Department had a well-defined plan and practiced it routinely; committed to train to the plan and use it as a foundation for response; established a culture of cooperation between their town and surrounding agencies; and made NIMS training available to all city agencies.

The report notes that AFD shift commanders are required to prepare and complete a NIMS I-204 form at the beginning of every shift. The form is an assignment listing and a fundamental part of a written Incident Action Plan (IAP). By requiring the shift commander to have an I-204 completed in advance, the formal written IAP process had already been set in motion at the time of the fire, a practice that helped the Apex Fire Department move from a local response to one that involved many mutual-aid agencies. The full technical report is available at http://www.usfa.dhs.gov/downloads/pdf/publications/tr_163.pdf.

NIOSH Safe Driving Report

In March 2008, a 33-year-old Emergency Services Sector (ESS) member was fatally injured after the tanker truck he was driving left the roadway and overturned. The victim, en route to a structure fire, took an unfamiliar route, and failed to negotiate a 90° curve to the right. The tanker left the roadway, rolled onto the driver's side, then slid through a ditch into a row of pine trees, crushing the cab.

The firefighter, a 12-year veteran of his department, was wearing his seatbelt, had recently completed a driver training renewal program, and routinely drove and operated the tanker (that had been inspected the previous month) under emergency conditions. The National Institute of Occupational Safety and Health (NIOSH) conducted an investigation of the fatal accident.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) examined the NIOSH report, "Volunteer Firefighter Dies in a Tanker Crash – Louisiana" (Firefighter Fatality Investigation # F2008-10), released in September.

In the report, NIOSH investigators reached the following conclusions intended to further protect the personnel and physical assets of fire service departments and agencies:

- Ensure tankers are driven at a safe and reasonable speed.
- Ensure responders are familiar with the location of the roads in their coverage areas.
- Consider staffing tankers with a minimum of two firefighters.
- Consider supplying responding units with maps or verbal directions to incident scenes, using computer-aided dispatch (CAD) or a global positioning system (GPS) device.
- Develop oversight of preventive maintenance programs for fire apparatus.
- Consider additional driver training for firefighters on safe tanker driving and operations.
- Ensure tankers meet all the requirements of National Fire Protection Association (NFPA) 1901, Standard for Automotive Fire Apparatus.

To view and download the full report, go to <http://www.cdc.gov/niosh/fire/reports/face200810.html>.

Municipal Water Supply Systems

The U.S. Fire Administration (USFA) recently completed a project with the Society of Fire Protection Engineers (SFPE) Educational & Scientific Foundation to enhance effective fire protection. The project team studied and evaluated the latest trends and technologies related to municipal water supply systems. The endeavor was conducted with support of the Department of Homeland Security (DHS) Science and Technology Directorate.

“This initiative will be of value to local-level fire protection, supporting USFA’s goal to reduce the loss of life and property from fire,” said U.S. Fire Administrator Greg Cade. “This cooperative effort allows communities to have comprehensive information on the latest technologies in municipal water supply systems in support of fire suppression activities and concerns.”

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) noted that the project team examined issues of interoperability and Critical Infrastructure Protection, as well as backup and redundant water supply systems for fire protection. From their analysis, the team created two reports: Volume 1—Water Supply Systems Concepts, and Volume 2—Water Supply System Evaluation Methods.

Both reports are available for download, free of charge, from the USFA web site at:

http://www.usfa.dhs.gov/fireservice/research/dsn/dsn_waterstudy.shtm.

Cyber Security Awareness Month

Communication/cyber systems are among the critical infrastructures of the Emergency Services Sector (ESS), and as the fifth annual observance of National Cyber Security Awareness Month begins, the Department of Homeland Security (DHS) is reinforcing the importance of protecting computers in workplaces and in the nation’s critical infrastructures, a practice particularly applicable to the country’s 9-1-1 centers and automated emergency dispatch systems.

The National Cyber Security Alliance (NCSA), one of the groups promoting National Cyber Security Awareness Month, considers up-to-date antivirus, antispyware, and firewall software a minimum level of protection. However, NCSA’s executive director cautions that, “Computer users are using the Web to do more things at the same time that online criminals are launching more sophisticated attacks...that puts a significant responsibility on computer users to be aware of cyber attacks, including online scams and fraud schemes.” Responder organizations’ increasing reliance on cyber systems includes purchasing physical assets via the Internet.

As the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) has written in previous INFOGRAMs, ESS personnel are encouraged to change passwords regularly and back up important files, but not to provide personal information to senders of unsolicited e-mail and to check whether a web site needs personal information before giving it. Ensuring that secured web sites start with <https://> rather than <http://> is another proactive practice.

DHS offers a variety of materials to encourage more secure cyber systems, including safe computing tips, fact sheet, and downloadable flyer, at <https://dhsonline.dhs.gov/portal/jhtml/dc/sf.jhtml?doid=117252>. Additional tips can be found at the web site of the U.S. Computer Emergency Readiness Team (US-CERT), <http://www.us-cert.gov>. For practical information on how to guard against Internet fraud, protect personal information, and increase computer security, log on to <http://www.onguardonline.org/#>.

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