



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

**INFOGRAM 30-08**

**August 7, 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](mailto:emr-isac@dhs.gov).*

### CIP Plan Development

The 2<sup>nd</sup> edition of the Critical Infrastructure Protection (CIP) Process Job Aid can be seen at <http://www.usfa.dhs.gov/downloads/pdf/publications/fa-313.pdf> (4.55 MB, 32 pages). In chapter 6 of this document (Establishing a CIP Program), the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) provides justification for a quality CIP Program: "...supports the protection or resiliency of the people, physical assets, and communication/cyber systems upon which survivability, continuity of operations, response-ability, and mission accomplishment depend." The EMR-ISAC submits that this justification is central to the mission of any state or municipality within the United States, and must be sustained by a superlative plan. The plan should enhance the protection and resiliency of state and local critical infrastructures to guarantee the maintenance of vital governmental missions, services, and economic functions during and after a man-made or natural disaster.

When searching for a good example of a CIP plan, the EMR-ISAC found the recently released Commonwealth of Virginia Critical Infrastructure Protection and Resiliency Strategic Plan. Also known as the "Virginia Plan," it clearly defines the Commonwealth's strategy to protect critical infrastructures and key resources, "so that essential state services and economic functions continue during a terrorist attack, a natural disaster or other type of significant incident."

Review of the "Virginia Plan" substantiates that it adheres to the National Infrastructure Protection Plan by ensuring the effective use of federal funding and resources to mitigate the effects of any emergency. The Plan tasks the Office of Commonwealth Preparedness to work with local, state, and federal officials as well as the private sector to coordinate the strategy along with its supporting implementation plans.

Because it offers a seamless, coordinated security and preparedness approach to infrastructure protection and resiliency, the EMR-ISAC recommends examination of the "Virginia Plan" by any state or municipality considering CIP plan development. The Plan is available at the following web site: [http://www.ocp.virginia.gov/Initiatives/documents/VA\\_Plan.pdf](http://www.ocp.virginia.gov/Initiatives/documents/VA_Plan.pdf) (1.78 MB, 42 pages).

### Protecting the Protectors

It is widely accepted throughout the United States that Emergency Services Sector (ESS) departments and agencies are the first line of defense within the nation. While America's military combats terrorism on foreign soils, local first responders are actively preventing, protecting, and responding to various forms of terrorism at home. Much too often, many challenges and personal risks confront ESS personnel when performing essential services for their respective communities.

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) learned of a recent incident in which police attempted to serve a search warrant at a local residence. When peering inside the home, the officers saw a methamphetamine lab with 16 large gas cylinders. Even worse was their observation of a probable explosive device. After the arrival of the fire department, emergency medical technicians, and hazmat, the makeshift electrical and alarm systems were dismantled. The cylinders containing anhydrous ammonia gas were determined to be too dangerous to transport and were destroyed at the scene.

EMR-ISAC research concludes that meth labs, drug trafficking, and narco-terrorism have become a very real type of chemical warfare that first responders must combat with increasing frequency. Consequently, too many ESS personnel are the community's soldiers actively engaged in the drug war. For example, meth labs can explode because of the volatile chemicals used in the production process. The toxicity of the chemicals can transform a neighborhood into a dangerously contaminated area. Additionally, the chemicals can potentially seep through cracks in chemical-protection suits worn by hazmat teams.

These realities warrant an aggressive training program to ensure the protection of the protectors. Therefore, the EMR-ISAC suggests that emergency personnel be taught to enforce the following prohibitions when dealing with any illicit labs (regardless of location) containing any type of chemicals: DO NOT taste, touch, smell, pour, jiggle, smoke, operate light switches, plug or unplug anything electrical, rub eyes or nose or mouth, forget about booby traps, remain longer than absolutely necessary, or hesitate to call the hazmat team.

More information about responder safety and heeding the warning signs of chemical manufacture can be seen at the following link: <http://www.respondersafety-digital.com/respondersafety/200709/?pg=3>.

## National Guard JISCC

The National Guard's Joint Incident Site Communications Capability (JISCC) quickly establishes interoperable communications for major Emergency Services Sector (ESS) response operations. In most cases, JISCC teams are capable of responding on scene within six hours of a serious event. With communication/cyber systems one of the three most critical ESS infrastructures, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) views JISCC systems as a considerable multiplier of vital resources.

A JISCC is a mobile communications system that can be towed or airlifted to incident sites to provide communications in the aftermath of disasters when existing communications systems are often degraded or destroyed. Its 33-foot antenna allows communication over high frequency, ultra high frequency, very high frequency, and 800 MHz channels. The system's array of computer and communications equipment enables emergency responders to communicate with each other even if they use different systems, by interfacing radio systems, cell phones, and landlines. Typically, within an hour of arriving on scene, it provides voice, data, video, and radio links between and among responder departments and other local, state, and federal agencies.

During the 2006 hurricane season, a minimum of one JISCC deployable communications system was fielded in each of the hurricane-prone states in the southeastern United States. Between October 2004 and June 2008, the National Guard Bureau's Communications Directorate fielded 72 JISCC systems. The Directorate's goal is to have at least one JISCC in each U.S. state and territory.

The JISCC is one of many National Guard capabilities helpful to the ESS. Others include Reaction Forces trained to provide governors or combatant commanders with rapid protection of critical infrastructures or other missions as directed to promote stability and security in the states, territories, and nation; Civil Support Teams that can identify chemical, biological, radiological, and nuclear (CBRN) agents and substances; and, CBRN+ high-yield Explosive (CBRNE) Enhanced Response Force Packages. For additional information about the programs, visit <http://www.ngb.army.mil/features/HomelandDefense/cip-maa/index.html>. To view an article on the JISCC, see [http://www.ngb.army.mil/news/archives/2008/07/073008-Guard\\_capability.aspx](http://www.ngb.army.mil/news/archives/2008/07/073008-Guard_capability.aspx).

## National Emergency Communications Plan

The Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) reviewed the just-released Department of Homeland Security (DHS) National Emergency Communications Plan (NECP), the nation's first strategic plan to enable long-needed interoperable communications among Emergency Services Sector (ESS) departments and agencies and with government officials. To ensure the needs and requirements of ESS communication/cyber systems were appropriately reflected in the plan, the DHS Office of Emergency Communications (OEC) worked with more than 150 public and private sector communications officials.

The NECP aims to make improvements at all levels of government in technology, coordination, governance, planning, usage, training, and exercises. It provides recommended initiatives and milestones to guide the improvements, but does not dictate the distribution of homeland security funds. Communications investments are among the most significant, substantial, and long-lasting capital investments that agencies make, the plan states, and emergency communications technological innovations evolve rapidly. Therefore, according to the plan, "DHS recognizes that the emergency response community will, over time, realize this national vision in stages, as agencies invest in new communications systems and as new technologies emerge." The NECP will be used to identify and prioritize investments to move the nation toward the vision.

The plan sets three milestone dates (supported by seven objectives) for achieving the high-level goal of establishing a minimum level of interoperable communications: "Demonstrate response-level emergency communications (the capacity of individuals with primary operational leadership responsibility to manage resources and make timely decisions during a multi-agency incident without technical or procedural impediments) within {a designated time period} for routine events involving multiple jurisdictions and agencies."

1. Goal 1: By 2010, 90 percent of all high-risk Urban Areas designated within the Urban Area Security Initiative (UASI) will meet the goal within one hour for routine events.
2. Goal 2: By 2011, 75 percent of non-UASI jurisdictions will meet the goal within one hour for routine events.
3. Goal 3: By 2013, 75 percent of all jurisdictions will meet the goal within three hours of a significant event.

The NECP will not supplant the Statewide Communication Interoperability Plans (SCIPs) recently approved by DHS for all U.S. states and territories. Instead the SCIPs will be updated to align with the goals of the plan through grant programs administered by DHS, including the new Interoperable Emergency Communications Grant Program.

For additional information about the NECP and OEC, contact [OEC@hq.dhs.gov](mailto:OEC@hq.dhs.gov). The plan can be seen at [http://www.dhs.gov/xlibrary/assets/national\\_emergency\\_communications\\_plan.pdf](http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf) (4.1 MB, 83 pages).

### **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](mailto: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](mailto:emr-isac@dhs.gov), fax: 301-447- 1034,  
Web: [www.usfa.dhs.gov/subjects/emr-isac](http://www.usfa.dhs.gov/subjects/emr-isac), Mail: J-247, 16825 South Seton Avenue,  
Emmitsburg, MD 21727