

## **NIMS: Information Sharing for Results**

*By Lieutenant David J. Mulholland, U.S. Park Police, Washington, D.C.*

**A**re you a law enforcement executive interested in getting a piece of the recently released \$1 billion in public safety interoperability grants (PSIGs)? Maybe you are considering a different Department of Homeland Security or Department of Justice block grant. Perhaps you are a law enforcement executive who is not looking to the federal government for grant funding but still has an interest in enabling the sharing of information among all primary and secondary responders during an incident response. If so, you now have a compelling interest in the National Incident Management System (NIMS).

In February 2003, U.S. president George W. Bush issued a Homeland Security Presidential Directive (HSPD-5) on the management of domestic incidents. The purpose of HSPD-5 is to “enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.” HSPD-5 directed the Department of Homeland Security to develop NIMS, which has been defined as a system that would “include a core set of concepts, principles, terminology, and technologies covering the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources.”<sup>1</sup> HSPD-5 also directed that all federal agencies begin using NIMS upon its publication and that, beginning in fiscal year 2005, NIMS compliance would become a prerequisite for state, local, and tribal public safety agencies to receive grant funding. Law enforcement officials who desire to benefit from a wide range of future funding opportunities must increase their knowledge of NIMS and the compliance of their agency information systems to NIMS specifications.

### **Information Sharing during an Incident**

NIMS provides principles to organize incident response in a uniform manner (the Incident Command System), collect and share information during an incident (multiagency coordination systems), and notify the public before and during an incident (public information systems).

Law enforcement executives should look to the NIMS principles to ensure that information systems used during incident response allow for real-time information flows between participating agencies during an incident to develop a “common operating

picture” available to all jurisdictions’ disciplines. In addition to ensuring that field personnel and decision makers have a good understanding during the incident of all events that are occurring, an information-sharing system based on NIMS principles should both enable the collection and sharing of intelligence and sensitive information securely and provide information to public information officers to inform or warn the community as appropriate.

## **Core Requirements of NIMS**

It is critical for a law enforcement executive to have a system in place that allows for the exchange of information (data) that meets NIMS requirements for information sharing. During an incident, or in preparation for an incident, data-sharing systems must be established that facilitate the exchange of real-time information, including across disciplines (police, fire, EMS, and transportation) and across jurisdictions. Real-time information, flowing freely and accessible by all stakeholders, is necessary to provide situational awareness for responders either in the field or at incident command centers.

A properly organized system permits incident commanders to provide strategic direction across all agencies involved in a response. These systems must be exercised and utilized during routine calls for service so that they may be easily implemented and managed during large-scale unexpected crisis events.

Real-time sharing of information is critical to incident commanders and responders, but it presents challenges such as ensuring that shared information is accurate. The information-sharing system should have a procedure to inform participants of the validity of any available information.

The system must facilitate the sharing of information using common terminology as defined in the Incident Command System and common language, so that there is no misinterpretation or confusion among disperse responding and participating agencies. Additionally, the system should facilitate information sharing with nongovernmental agencies—“nontraditional” secondary responders critical to incident response such as the American Red Cross, public utility companies, and so on.

To ensure that information is shared in a secure environment, the system must identify and authenticate users and allow them access only to the appropriate level of information, segregating law enforcement information from the general view and intelligence information from noncleared or nonvetted personnel.

The system should leverage current information-sharing standards such as the National Information Exchange Model (NIEM) and the Emergency Data Exchange Language (EXDL), to name a few. The system should also incorporate the ability to import and utilize geospatial information.

Finally, the system should integrate with appropriate emergency operation centers (EOCs) and Joint Information Centers (JICs). JICs are clearinghouses within the NIMS structure designed primarily for facilitating information dissemination to the public through the public information officers whose agencies are involved in the incident.

## **CapWIN: A Case Study**

The IACP recently conducted a comprehensive review of the Capital Wireless Information Net (CapWIN) to determine the level and extent that CapWIN met NIMS requirements. The CapWIN network is an incident management and information-sharing

system in which over 35 agencies in the District of Columbia, Maryland, and Virginia participate. The analysis has shown that the system meets a great majority of the NIMS requirements. CapWIN provides the ability to post documents such as incident action plans (IAPs), emergency operation plans (EOPs), maps, resource listings and locations, and NIMS forms. Additionally, the system has the ability to export the incident data log directly into the NIMS-formatted incident log (ICS-214). Recommendations were made for minimal changes in nomenclatures to select fields to achieve NIMS common terminology. Agencies in the District of Columbia, Maryland, and Virginia can now look to CapWIN as a tool for achieving the informationsharing requirements of NIMS.

## **Conclusion**

Law enforcement executives are encouraged to review their current systems that manage and enable information exchange between agencies during incidents to determine whether those systems fulfill the principles of NIMS. Executives considering procurement or adoption of information systems designed for incident response should closely examine whether those systems comply with NIMS principles. More information regarding NIMS can be found at the National Integration Center's Web site at <http://www.fema.gov/emergency/nims/index.shtm> or at <http://www.nimsonline.com> ■

## **Note:**

<sup>1</sup>White House, "Homeland Security Presidential Directive/HSPD-5," press release, February 28, 2003, <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html> (accessed October 3, 2007).

[Top](#)

From The Police Chief, vol. 74, no. 11, November 2007. Copyright held by the International Association of Chiefs of Police, 515 North Washington Street, Alexandria, VA 22314 USA.