NIMS *Guide*

NG 0004
January 10, 2008
Incident Management Systems
202-646-3850

National Incident Management System (NIMS) Communications and Information Management Standards

Purpose of the Guide:

This NIMS *Guide* provides a brief overview of five recommended standards that support NIMS implementation. Through evaluation and practitioner review conducted in 2007, the Incident Management Systems Division (IMSD) has identified and recommends that emergency management/response organizations and private sector vendors voluntarily adopt the following five standards, which support interoperability among communications and information management systems:

- ANSI INCITS 398-2005: Information Technology – Common Biometric Exchange Formats Framework (CBEFF)
- IEEE 1512-2006: Standard for Common Incident Management Message Sets for Use by Emergency Management Centers
- NFPA 1221: Standard for Installation, Maintenance, and Use of Emergency Services Communications Systems
- OASIS Common Alerting Protocol (CAP) v1.1
- OASIS Emergency Data Exchange Language (EDXL) Distribution Element v1.0

Common interfaces among disparate communications and data management systems is needed to integrate information into a common operating picture, facilitating decision making during an incident. Applicability to NIMS includes the following elements.

- Incident communications are facilitated through the development and use of common communications plans, interoperable communications equipment, processes, standards, and architectures.
- Communications and data standards (and related testing) and associated compliance mechanisms are necessary to enable diverse organizations to work together effectively.

In FY 2008, compliance activities are linked to the standardization of data and information management processes.

Private sector vendors have a responsibility to integrate standards into their communications and information management products. Similarly, government officials should reference the appropriate standards when purchasing hardware and software off-the-shelf, and identify them in Requests for Proposals (RFPs) during the development of original products. The following pages provide an overview of the five information management standards, a description of their relationship to NIMS, and contact information for the standards development organizations. Most standards are available for download free of charge or downloaded or purchased for a fee on the respective organization's Web site.

NIMS *Guide*

NG 0004
January 10, 2008
Incident Management Systems
202-646-3850

American National Standards Institute (ANSI) INCITS 398-2005 Information Technology – Common Biometric Exchange Formats Framework (CBEFF)

1. **Overview:** The Common Biometric Exchange Formats Framework (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data elements can be placed in a single file used to exchange biometric information between different system components or between systems themselves. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange. Specifically, ANSI INCITS 398-2005 supports multiple biometric data types (e.g., fingerprint, face and voice recognition, etc.) and/or multiple biometric data blocks of the same biometric type. It also defines biometric data objects for use within smart cards and other tokens and describes common fields for biometric features and the validity period.

2. **Relationship to NIMS:** The sharing of biometric data may be used in a number of different ways within the communications and information management component of NIMS. The use of digital biometric data is becoming a common characteristic of credentialing and badging systems for identification that allows access to an incident scene by the proper agents. The use of digital biometric information to verify the identity of emergency management/response officials is becoming commonplace; ANSI INCITS 398-2005 serves as a way for responders to standardize use and exchange of biometric data.

   The sharing of biometric data may also be useful to the Facilities Unit and Medical Unit as part of the Incident Command System (ICS). Biometric information may be collected and shared among emergency management/response organizations for purposes of identifying displaced persons needing housing and care or victims of an incident, such as a pandemic influenza. In summary, this standard establishes a common format for compiling and exchanging biometric information during and after an incident.

Standard Development Organization: InterNational Committee for Information Technology Standards (INCITS)
Technical Committee: INCITS/M1, Biometrics Technical Committee
Standard Designation and Edition: INCITS 398-2005[1]
Web site: www.ansi.org (to purchase this standard)

[1] Standard is currently under revision. Contact INCITS for further details.

NIMS *Guide*

Institute of Electrical and Electronics Engineers (IEEE) 1512, 1512.1, 1512.2, and 1512.3: Standards for Common Incident Management Message Sets for Use by Emergency Management Centers[2]

1. **Overview:** This family of standards addresses the exchange of data on transportation-related incidents above the field level for Emergency Operations Centers (EOCs) and other Multi-Agency Coordination Systems (MACS) components. These standards utilize message sets that are described using Abstract Syntax Notation One ("ASN.1") Syntax or XML formats. The standard provides definitions, specific messages, data frames, and data elements for communicating information for use by EOCs in real-time for interagency transportation-related incidents. IEEE 1512 is the baseline document for standards 1512.1, 1512.2, and 1512.3, which relate to traffic incidents, public safety, and hazardous cargo, respectively. As the baseline document it establishes the requirements for all EOCs, and it provides a benchmark for operations, communications, and relationships between the EOC and other emergency management/response organizations involved in traffic-related incidents.

2. **Relationship to NIMS:** The IEEE suite of standards directly supports the operation of MACS and EOCs and provides a benchmark for information and data exchange above the field level for transportation-related incidents, including hazardous material spills. These standards help define the relationships among various public safety disciplines, including transportation, law enforcement, and fire. In summary, the IEEE standards establish a uniform framework for data sharing between agencies and jurisdictions to support the establishment of a common operating picture during transportation-related incidents.

Standard Development Organization: Institute of Electrical and Electronics Engineers (IEEE)
Technical Committee: IEEE Standards Coordinating Committee 32, sponsored by the Intelligent Transportation Systems Committee of the IEEE Vehicular Technology Society
Edition Number and Date: 1512-2006, 1512.1-2006, 1512.2-2004, 1512.3-2006
Web site: www.ieee.org

NIMS GUIDE reprinted with permission from IEEE Standard 1512-2006; Standard for Common Incident Management Message Sets for Use by Emergency Management Centers to incorporate the information in Federal Emergency Management Agency (FEMA) NIMS (National Incident Management System) Guides published under the auspice of the federal Department of Homeland Security (DHS), Copyright 2006*, by IEEE. The IEEE disclaims any responsibility or liability resulting from the placement and use in the described manner.*

[2] From IEEE Standard 1512-2006. Copyright 2006 by IEEE. All rights reserved.

NIMS *Guide*

NG 0004
January 10, 2008
Incident Management Systems
202-646-3850

National Fire Protection Association (NFPA) 1221: Standard for Installation, Maintenance, and Use of Emergency Services Communications Systems

1. **Overview:** The NFPA 1221 standard covers the installation, performance, operation, and maintenance of public emergency services communications systems and facilities. It is not intended as a design specification manual or an instruction manual. The standard covers systems that receive alarms from the public, e.g., 9-1-1 services systems and communications centers, and retransmits those alarms to response agencies. It also provides requirements for dispatching systems and establishes a level of performance and the quality of installations for emergency communication systems. Elements of these systems may include communications centers, signal wiring, emergency response facilities, operations centers, telephones, dispatching systems, computer-aided dispatching, and public alerting systems. Other operations covered under this standard include system testing, record keeping, and network security.

2. **Relationship to NIMS:** NFPA 1221 supports the NIMS requirements for: interoperability; reliability, scalability, and portability; and resilience and redundancy among communications systems. The standard established a benchmark for communication equipment installation, maintenance, and testing/use, which are critical for ensuring that communications remain in place for emergency management/response personnel and to mitigate the chance of disruptions during an incident.

   NFPA 1221 supports the components of an interoperability plan by requiring that emergency services organizations develop policies and standard operating procedures on use of communications equipment. The standard ensures that communications equipment is properly functioning; it also benefits emergency management/response organizations in the following ways:
   - Preventive maintenance avoids high replacement costs for communications equipment.
   - The standard establishes baseline requirements for emergency dispatching systems.

Standard Development Organization: National Fire Protection Association (NFPA)
Technical Committee: Public Emergency Services Communications
Edition Number and Date: 2007
Web site: www.nfpa.org

NIMS *Guide*

NG 0004
January 10, 2008
Incident Management Systems
202-646-3850

Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol v1.1

1. **Overview:** The Common Alerting Protocol (CAP) is an international format for exchanging all-hazard emergency alerts and public warnings over a variety of networks. The CAP standard allows a consistent warning message to be disseminated simultaneously over many different warning systems, increasing the effectiveness and efficiency of the warning system. The CAP provides an open, non-proprietary digital message format that is compatible with existing and emerging formats. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as information about unique hazards or hostile acts.

2. **Relationship to NIMS:** "Successful communications and information management require that emergency management/response personnel and their affiliated organizations utilize standard communications types … [including] emergency alerts and warnings (Draft NIMS, August 2007)." The CAP standard supports the establishment of an integrated warning system; allowing the dissemination of a single warning or message through multiple devices by a single person with authority. By building products to the CAP standard, various warning devices or systems may be used to issue warnings and alerts to emergency responders and the public. For example, CAP messages may be sent and translated into: text for the mandated Emergency Alert System and captioning, amber alerts, digital voice formats for radios and telephones, and digital signals to activate sirens. Ultimately, the standard ensures that warnings and messages reach all emergency responders and citizens in an impacted area. Receiving the message through multiple mediums or channels will also increase the chance that citizens will take the appropriate action.

   The CAP standard supports the NIMS interoperability requirements by ensuring that:
   - Dissimilar alert and warning systems are compatible and that messages may be shared among them to reach citizens, emergency responders, and other affected organizations in an impacted area.
   - Emergency management/response personnel receive and exchange consistent messages and data on an incident, which supports the establishment of a common operating picture to facilitate decision making.

Standard Development Organization: Organization for the Advancement of Structured Information Standards (OASIS)
Technical Committee: OASIS Emergency Management TC
Edition Number and Date: Version 1.1, 2005
Web site: www.oasis-open.org

NIMS *Guide*

NG 0004
January 10, 2008
Incident Management Systems
202-646-3850

Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data Exchange Language (EDXL) Distribution Element v1.0

1. **Overview:** The EDXL Distribution Element (EDXL-DE) specification describes a standard message distribution structure for data sharing among emergency information systems using XML-based EDXL. This content based routing standard specifies to whom and under what circumstances the associated (enveloped) data is to be sent/received.

   The primary use of the EDXL-DE is to provide standardized routing assertions for all types of emergency data, whether it is an XML message, spreadsheet, jpeg image, or any other type of digital data.

2. **Relationship to NIMS:** The EDXL-DE content based routing standard is a powerful tool to support data interoperability among all types and levels of systems. The DE contains routing data as well as authentication, authorization, and security data about the data being routed. By building products using this routing standard, various systems and "systems of systems" can exchange data about an incident. For example, a CAP message may be sent to a targeted audience as a payload using EDXL-DE. The DE may be used to send supporting data about an incident. Ultimately, the standard ensures that warnings and emergency data reach impacted emergency responders and citizens in a timely manner. Receiving appropriate, targeted information about an incident will increase the chance that citizens will take the appropriate action and supports the establishment of a common operating picture to facilitate decision making.

Standard Development Organization: Organization for the Advancement of Structured Information Standards (OASIS)
Technical Committee: OASIS Emergency Management TC
Edition Number and Date: Version 1.0, 2006
Web site: www.oasis-open.org