

## **NIMS RECOMMENDED STANDARDS LIST (RSL)**

January 10, 2008

A fundamental responsibility of the FEMA's Incident Management Systems Integration (IMSI) Division is to identify guidelines, protocols, and standards that will help emergency managers and responders from all levels of the public and private sectors organize effective responses to emergency incidents and planned events. In support of that mandate, IMSI produces an annual Recommended Standards List (RSL) that describes voluntary consensus standards that support the implementation of the National Incident Management System (NIMS).

IMSI's standard review methodology includes an evaluation against NIMS criteria, followed by practitioner review. Part of the evaluation is a crosswalk between evaluated standards and the concepts, principles, and requirements in the most current publication of the NIMS (FEMA 501) document. IMSI relies on groups of subject matter experts to examine how the adoption of existing voluntary consensus standards would benefit NIMS implementation and impact the NIMS user community. This evaluation culminates in practitioner recommendations representing various emergency response disciplines.

The IMSI refers to these recommendations when developing the RSL each year, and encourages emergency management/response organizations to adopt standards on the RSL as part of NIMS implementation.

Previously recommended for voluntary adoption are the following two programmatic and incident management standards – NFPA 1600 (Disaster Emergency Management and Business Continuity Programs) and NFPA 1561 (Emergency Services Incident Management Systems).

The most recent iteration of the IMSD standards evaluation process placed priority on communications and information sharing/management. Integrating information into a common operating picture requires common interfaces among disparate communications and data management systems to facilitate decision making during an incident. These interfaces are established through the development and use of common communications plans, interoperable communications equipment, processes, standards, and architectures.

The following standards comprise the NIMS RSL:

### **Preparedness and Incident Management Standards**

- **National Fire Protection Association (NFPA) 1600: Standard on Disaster/Emergency Management and Business Continuity Programs**

**Overview:** This standard establishes a common set of criteria for disaster/emergency management and business continuity programs. Specifically, this standard provides disaster/emergency management and business continuity programs the criteria to assess current programs or to develop, implement, and maintain aspects for prevention, mitigation, preparation, response, and recovery from emergencies. This standard applies to public, nongovernmental, and private entities.

**Standard Development Organization:** National Fire Protection Association (NFPA)

**Technical Committee:** Emergency Management and Business Continuity

**Edition Number and/or Date:** 2007 Edition

Web site: <http://www.nfpa.org>

- **National Fire Protection Association (NFPA) 1561: Standard on Emergency Services Incident Management System**

**Overview:** This standard establishes the minimum requirements for an incident management system to be used by emergency services to manage all incidents/planned events. Requirements are established for operating systems, implementation, and communications. Furthermore, the standard provides a description of key positions and roles within the incident management system, including the functions of the Incident Commander, Command Staff, Operations, Planning, Logistics, and Finance/Administration. The standard also addresses requirements for multi-agency coordination and training and staffing for Incident Management Teams.

**Standard Development Organization:** National Fire Protection Association (NFPA)

**Technical Committee:** Fire Service Occupational Safety and Health

**Edition Number and/or Date:** 2005 Edition

**Web site:** <http://www.nfpa.org>

## Communications and Information Management Standards

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

**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.

**Standard Development Organization:** InterNational Committee for Information Technology Standards (INCITS)

**Technical Committee:** INCITS/M1, Biometrics Technical Committee

**Standard Designation and Edition:** INCITS 398-2005<sup>1</sup>

**Web site:** [www.ansi.org](http://www.ansi.org) (to purchase this standard)

---

<sup>1</sup> Standard is currently under revision. Contact INCITS for further details.

- **Institute of Electrical and Electronics Engineers (IEEE) 1512-2006: Standard for Common Incident Management Message Sets for Use by Emergency Management Centers**

**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.

**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

**Web site:** [www.ieee.org](http://www.ieee.org)

*From IEEE Standard 1512-2006. Copyright 2006 by IEEE. All rights reserved.*

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

**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, network security, and redundancy.

**Standard Development Organization:** National Fire Protection Association (NFPA)

**Technical Committee:** Public Emergency Services Communications

**Edition Number and Date:** 2007

**Web site:** [www.nfpa.org](http://www.nfpa.org)

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

**Overview:** The Common Alerting Protocol (CAP) is a general 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.

**Standard Development Organization:** Organization for the Advancement of Structured Information Standards (OASIS)

**Technical Committee:** OASIS Emergency Management Technical Committee

**Edition Number and Date:** Version 1.1, 2005

**Web site:** [www.oasis-open.org](http://www.oasis-open.org)

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

**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.

**Standard Development Organization:** Organization for the Advancement of Structured Information Standards (OASIS)

**Technical Committee:** OASIS Emergency Management Technical Committee

**Edition Number and Date:** Version 1.0, 2006

**Web site:** [www.oasis-open.org](http://www.oasis-open.org)