NIMS *Guide*

NG 0006
July 2008
National Preparedness Directorate
National Integration Center
Incident Management Systems Integration
202-646-3850

General Standards Overview

Introduction

FEMA's National Preparedness Directorate (NPD) through the National Integration Center (NIC) and the Incident Management Systems Integration Division (IMSI), manages the National Incident Management System (NIMS) and provides guidance material, such as this NIMS Guide, to the emergency management and response community to assist with the advancement and implementation of NIMS nationwide.

This General Standards Overview provides information on the development and use of standards in support of NIMS. The document contains information intended to foster a general understanding of standards as well as their importance in implementing NIMS.

The following sections define the various types of standards and the processes for their development and use, describe the role of standards development organizations (SDOs), and provide information on NPD initiatives and products.

Why are standards an important part of NIMS implementation?

While NIMS provides a common structure and terminology for responding to incidents and planned events, voluntary consensus standards support NIMS implementation by creating uniformity of use and practice. This support is particularly important for interoperable communications and integrated information management systems. Standards also provide:

- Accepted and uniform criteria for measuring the adequacy of preparedness efforts and performance of emergency operations;
- Technical guidance; and
- Common resource descriptions to facilitate mutual aid – the sharing of resources among jurisdictions.

What role does NPD and the Department of Homeland Security (DHS) play in the identification of NIMS Recommended Standards and DHS National Standards?

The NIC is responsible for designating standards appropriate for NIMS users in coordination with recognized standards development organizations (SDOs). Through the work of IMSI, the NIC monitors the development of standards and maintains the NIMS Recommended Standards List (RSL). IMSI may further recommend a NIMS standard to the DHS Science and Technology Directorate (DHS S&T) for consideration and adoption as a DHS National Standard.

DHS seeks the adoption of non-government standards over government-unique standards whenever possible and appropriate. DHS National Standards are not mandatory. However, their use by DHS components and customers, product manufacturers, and process developers is strongly encouraged.

Federally-mandated standards, such as the Federal Geospatial Data Committee Standards and Federal Information Processing Standards, are considered automatically adopted by DHS. Moreover, standards that have been referenced in OMB Circulars or in Executive Orders are considered adopted.

Types of Standards

How is a standard defined?

The Office of Management and Budget (OMB) Circular A-119 document defines standards as "common and repeated use of rules, conditions, guidelines, or characteristics for products or related processes and production methods and for related management systems practices."

What are voluntary consensus standards?

The strategy for the identification of NIMS-related standards primarily focuses on the identification and adoption of voluntary consensus standards. These standards are developed voluntarily by non-governmental entities independent of any government regulations or actions required by law. The National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) states that "[a]ll Federal agencies and departments shall use technical standards that are developed or adopted by voluntary consensus standards bodies." The following standards are not considered voluntary consensus standards:

- Company standards or other standards developed in the private sector but not through the full consensus process;
- Government-unique standards, which are developed by the government for its own uses but not through the full consensus process; or
- Standards mandated by law.

The term "voluntary consensus standard" is widely used among SDOs, industry, and government. The term "voluntary" means the standard is voluntarily developed and the decision to use it is also voluntary. However, once a voluntary consensus standard is placed in a contract, cited as a requirement, or required by law or regulation, compliance becomes mandatory, not voluntary. The term "consensus" has led to the misperception that 100 percent agreement is required before a standard is approved. Standards developers define consensus differently; in the area of standards, "consensus" typically means more than a simple majority but less than unanimous agreement.

What type of standards may be recommended for NIMS?

For NIMS purposes, NPD identifies, evaluates, and recommends voluntary consensus standards that may be grouped according to the following categories: system, operational, or technical standards. The following provides a brief definition and example of each type:

- System Standards identify and describe essential activities that facilitate communication and understanding of actions between organizations. System standards are often referred to as “process standards,” or “strategic standards.” Examples of system standards applications include communications networks, logistics, information systems, decision-making processes, preparedness activities such as training and education, and reporting systems.

- Operational Standards describe specific activities, or operations, that personnel at various levels of organizations may perform in the planning and execution of specific tasks or assignments. Operational standards are often referred to as “method standards” or “tactical standards.” Examples of operational standards include certain hazardous materials (HAZMAT) response protocols, incident-scene management procedures, radio/communications discipline, incident-scene safety procedures, and certain field sampling techniques.

- Technical Standards are standards that have common and repeated use of rules, conditions, guidelines or characteristics for products, processes and production methods, and related management systems practices. They also provide for the definition of terms; classification of components; delineation of procedures; and specification of dimensions, materials, performance, designs, or operations. Examples of technical standards include specifications for HAZMAT personnel protective equipment, guidelines for interoperable communications, and other emergency management and response equipment.

Standards Development Organizations

What is a Standards Development Organization (SDO) and how does it function?

An SDO, or standards body, is an entity whose primary activities include developing, coordinating, promulgating, and maintaining standards that address the needs of a broad base of users. These standards include provisions requiring that owners of intellectual properties related to the standards agree to make their information available on a non-discriminatory, royalty-free or reasonable royalty basis to all interested parties. Thus, SDO-promulgated standards are available to everyone and can usually be accessed and downloaded through an SDO’s Website.

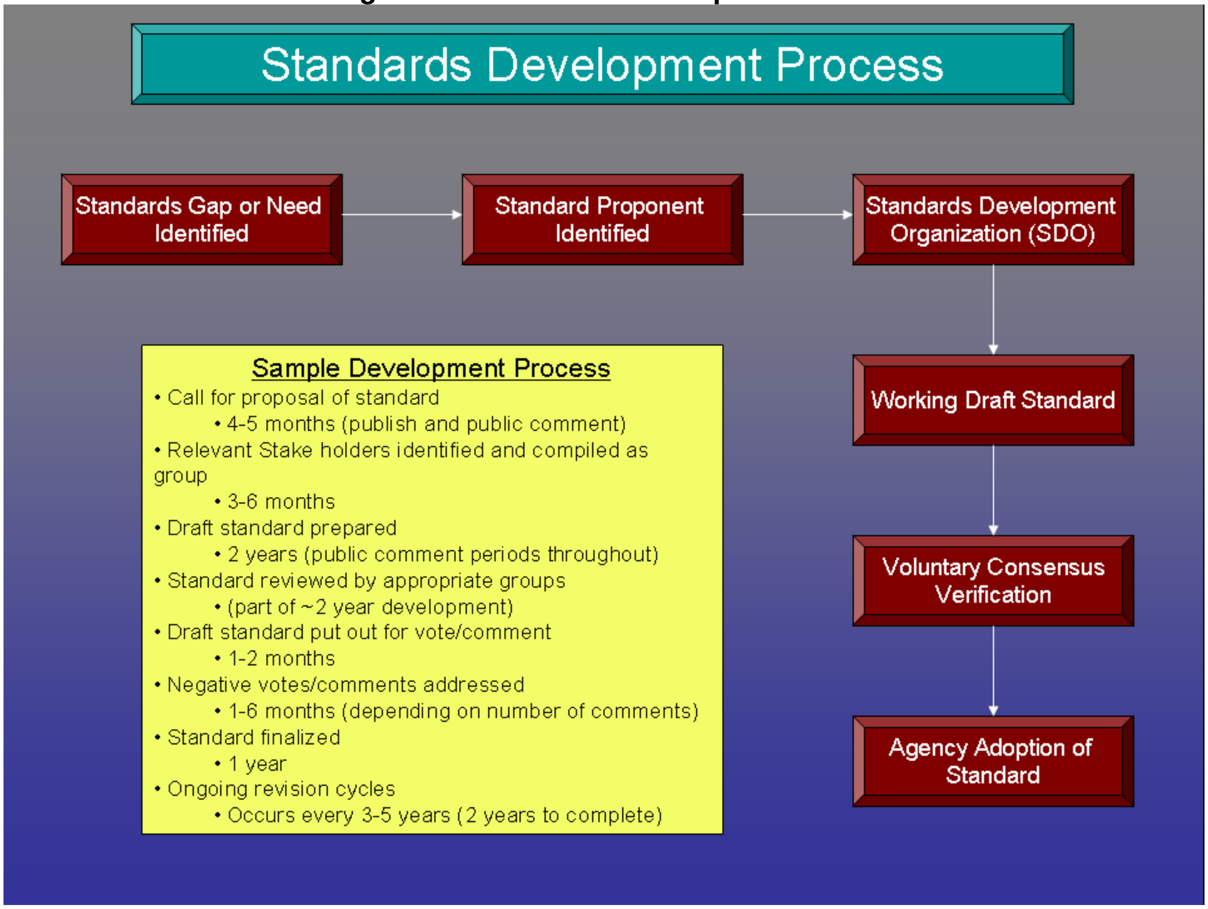
DHS Test & Evaluation and Standards Division considers ease of downloading access and reasonableness of SDO royalty fees when determining if a non-government standard should be adopted as a DHS National Standard.

How are standards developed by SDOs?

Figure 1, on the following page, shows how a common standard development process occurs. The red boxes reflect the major phases of an SDO’s voluntary consensus standards development process. The yellow box provides a more detailed timeline for the development of such standards.

As depicted in the first box, a standards gap or need is identified by an SDO or external stakeholders. The SDO identifies an appropriate standard proponent and issues a request or "call" for a Proposal of Standard. These steps, which include the drafting and publishing of the proposal and allowing for a period of public comment and revisions, may take up to four or five months.

Figure 1: Standards Development Process



Standards Development Process

Standards Gap or Need Identified

Standard Proponent Identified

Standards Development Organization (SDO)

Working Draft Standard

Voluntary Consensus Verification

Agency Adoption of Standard

Sample Development Process

- Call for proposal of standard
  - 4-5 months (publish and public comment)
- Relevant Stake holders identified and compiled as group
  - 3-6 months
- Draft standard prepared
  - 2 years (public comment periods throughout)
- Standard reviewed by appropriate groups
  - (part of ~2 year development)
- Draft standard put out for vote/comment
  - 1-2 months
- Negative votes/comments addressed
  - 1-6 months (depending on number of comments)
- Standard finalized
  - 1 year
- Ongoing revision cycles
  - Occurs every 3-5 years (2 years to complete)

The SDO next identifies relevant stakeholders to function as a working group to develop a working draft standard. This can cover an extended period of one to two years, and includes public and stakeholder review periods held throughout the drafting process.

Voluntary consensus verification requires the SDO to present the draft standard for vote and comment by an SDO designated voting committee. Negative votes and constructive comments will require further revision of the draft standard. As a result, this stage may require one to six months to complete.

Once the voting committee has approved the standard, the SDO finalizes the standard for posting. The SDO then announces the approved standard on their Website and other media and its availability for public use.

The SDO maintains the new standard by conducting revision cycles every three to five years. Revision of the standard includes committee-generated changes as well as changes suggested during public comment review.

The final step in the standard development process is agency adoption of the standard. Government, non-government, and private sector organizations may elect to further evaluate the standard for adoption and promulgation within their organization and user communities.

In the government arena, the standards adoption process for State and local government entities varies widely depending on the jurisdiction. In many cases, however, incentives exist for certification, accreditation, or adoption of standards. These incentives take many forms, such as: certification of equipment and people, grant-linked requirements for adoption of specific standards; reduced insurance and bonding rates; special recognition insignias reflecting compliance; and standards adopted as a part of an established accreditation process.

DHS maintains internal processes for the adoption of voluntary consensus standards as DHS National Standards. The Federal Government neither operates nor finances an official national standards body, notwithstanding the National Institute of Standards and Technology (NIST). However, with the strong support of SDOs, the Federal Government is an important player in the standards process as a user, regulator, and contributor.

Supporting Products

NPD is committed to providing informational materials and other guidance documents to the emergency management and response community to foster common understanding of NIMS-related standards activities. These products are posted on the FEMA Website to maximize information sharing. They include the publication of NIMS Alerts, NIMS Guides, the NIMS RSL, and reports of NIMS-related product evaluations.

What is a NIMS Alert?

NIMS Alerts are brief, typically one page, announcements created by the NIC and posted on the FEMA Website. They are intended to alert the emergency management and response community of important NIMS-related information and refer the reader to reference documents on the topic. The Alert may also advise that more detailed information will follow in a subsequent NIMS *Guide*.

What is a NIMS Guide?

A NIMS Guide provides summary information or guidance on NIMS-related topics. They are published by the NIC and posted on the FEMA Website for information sharing purposes. A NIMS Guide is typically developed for each standard on the RSL. The Guides provide general overviews of the standards as well as illustrate the standards' relationships to NIMS, and their benefits to incident management operations. NIMS Guides also provide information about accessing copies of standards and Website links to the respective SDO.

What is the NIMS Recommended Standards List (RSL)?

The NIMS RSL is a list of standards that have been approved by the NIC as suitable to support NIMS. All standards on the RSL have been evaluated by subject matter experts using a series of NIMS evaluation criteria to ensure their relevance and their value to NIMS. The RSL is updated by IMSI whenever a new standard is approved.

What is the NIMS Supporting Technology Evaluation Program (NIMS STEP)?

The NIMS Supporting Technology Evaluation Program (NIMS STEP) provides independent, objective evaluation of commercial and governmental products against NIMS standards, concepts, and principles. When applicable, communications and information management standards on the RSL are integrated into the NIMS STEP program. This provides users and vendors an opportunity to receive a “no cost” evaluation of a product for compliance with a NIMS standard.

A primary benefit to the emergency management and response community includes a list of product descriptions, key capabilities, and an evaluation report that may be accessed on the Responder Knowledge Base (RKB) Website (https://www.rkb.us/). Vendors benefit by receiving a copy of the NIMS STEP Evaluation Report which identifies areas for enhancement of their product.

NIMS STEP has been designed to evaluate products that support emergency managers and responders in decision-making prior to and during an incident. The types of products evaluated include the following:

- Vulnerability analysis, hazard forecasting, and consequence assessment;
- Intellegence and analysis;
- Physical and cyber security, access control, and surveillance;
- Collaboration;
- Incident management; and
- Communication and network infrastructure.

For additional information about the NIMS STEP program, visit: http://www.fema.gov/emergency/nims/nims_testing.shtm.

Website

More about the information referenced in this document can be found at the following Website: http://www.fema.gov/emergency/nims/standards.shtm.