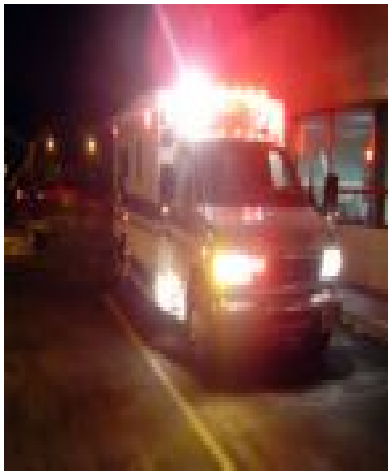
U.S. Department of Homeland Security's Emergency Interoperable Standards Efforts

Presented to the Workshop and Demonstration of Advances in Standards for Public Warning

Chip Hines, PMP
Program Manager, Disaster Management
Office for Interoperability and Compatibility
Science and Technology Directorate
October 19, 2006

Defining the Problem

Emergency responders often have difficulty exchanging voice and data communications when adjacent emergency response agencies are assigned to different radio bands, use incompatible proprietary systems and infrastructure, and lack adequate standard operating procedures and effective multi-jurisdictional, multi-disciplinary governance structures.



Effective communications can mean the difference between life and death.

Homeland Security

OIC Background

The Department of Homeland Security (DHS) established the Office for Interoperability and Compatibility (OIC) in 2004 to strengthen and integrate interoperability and compatibility efforts in order to improve local, tribal, state, and Federal emergency preparedness and response. Managed by the Science and Technology (S&T) Directorate, OIC is assisting in the coordination of interoperability efforts.

OIC programs and initiatives address critical interoperability and compatibility issues. Priority areas include communications, equipment, and training.

Homeland Security

Voice and Data Interoperability Programs

OIC's communications portfolio is currently comprised of the Disaster Management (DM) and SAFECOM programs.

DM is improving incident response and recovery by developing tools and messaging standards that help emergency responders manage incidents and exchange information in real time.

SAFECOM is creating the capacity for increased levels of interoperability by developing tools, best practices, and methodologies that emergency response agencies can put into effect immediately, based on feedback from emergency response practitioners.

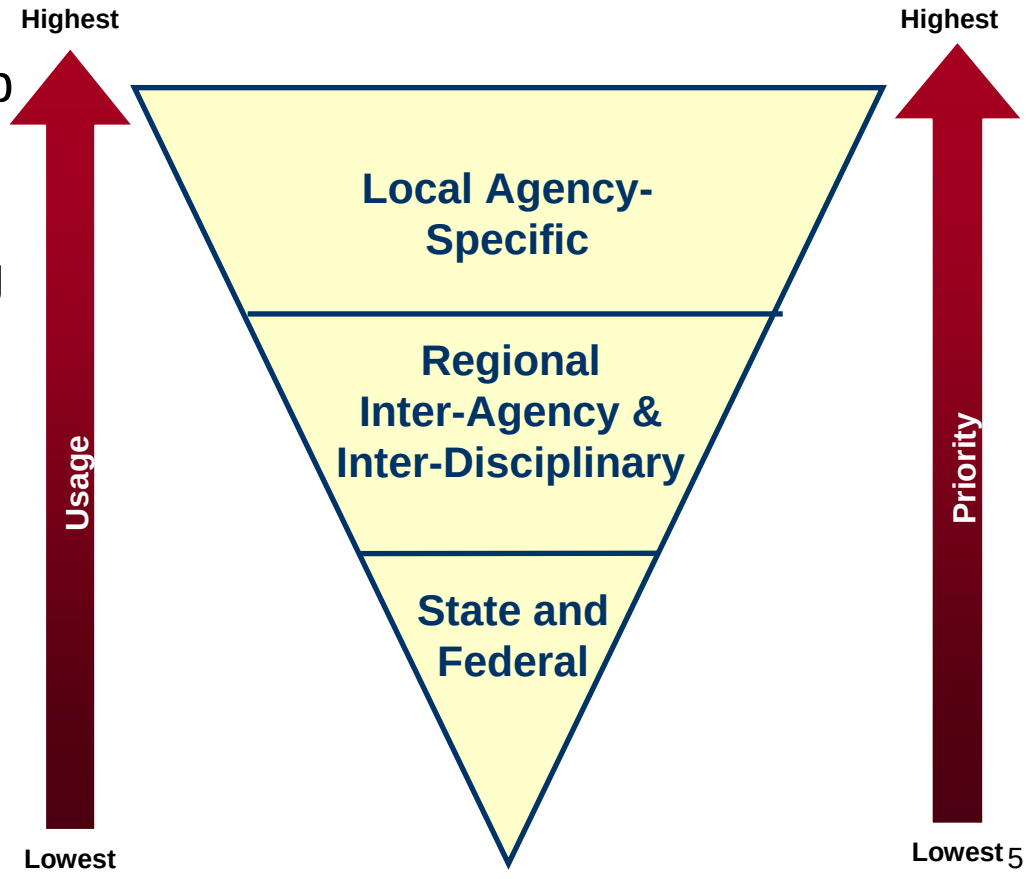
Together, DM and SAFECOM are providing state and local emergency responders with resources intended to address all aspects of communications interoperability.

Homeland Security

Practitioner-Driven Approach

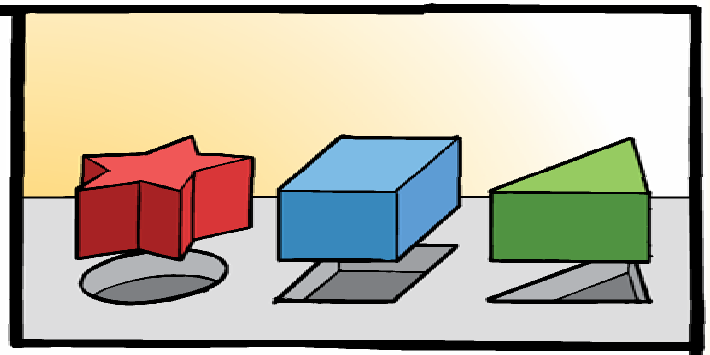
DM and SAFECOM both advocate a unique, “bottom-up” approach. The practitioner-driven governance structures benefit from the critical input of the emergency response community and from local, tribal, state, and Federal policy makers and leaders. This input ensures that OIC resources are aligned with state and local needs.

- DM’s Practitioner Steering Group (PSG) ensures that initiatives and tools effectively meet practitioners’ information-sharing priorities and requirements.
- SAFECOM’s Executive Committee and Emergency Response Council facilitate the input of emergency responders, policy makers, and leaders.



Homeland Security

Standards Development



The DM standards initiative is:

- A practitioner-driven effort to develop response operation messaging standards for sharing information.
- A public-private partnership to ensure industry includes standards in their systems and software.

Who Uses Standards?

- Emergency responders
- Industry

What does it do for me?

- Standards ensure the information emergency responders send and receive is understood by all parties and will produce the results and actions they intend. This concise exchange of data prevents confusion and errors during incidents.
- Standards operate behind the scenes and don't require additional effort from users
- Standards allow emergency responders using different software and systems to seamlessly share information.

Homeland Security

Need for Data Messaging Standards

Current State

- **There is a lack of data-sharing standards needed for emergency management software tools to share critical incident-related information.**
- **There is a perception that it is not possible to change every system/data to "speak the same electronic language."**

Future State

- **Emergency responders seamlessly share incident-related information.**
- **Information is displayed in a user-friendly format.**
- **Existing standardization efforts are leveraged.**
- **Requirements are practitioner driven.**

Messaging standards implementation drives data systems to interoperability. Compliant software can exchange and display information in their own native way.

Homeland Security

DM Standards Development

Emergency Data eXchange Language (EDXL)

- Suite of messaging standards with technical rules governing how incident-related information is packaged for exchange
- XML-based; not data standards; business process-driven
- Driven by practitioner-defined priorities and requirements

EDXL Implementation

- Software vendors update products to receive and send information using these standards.
- OPEN Application Programming Interfaces are free to use.
- DM works closely with the vendor community to ensure that resulting standards are implemented effectively.

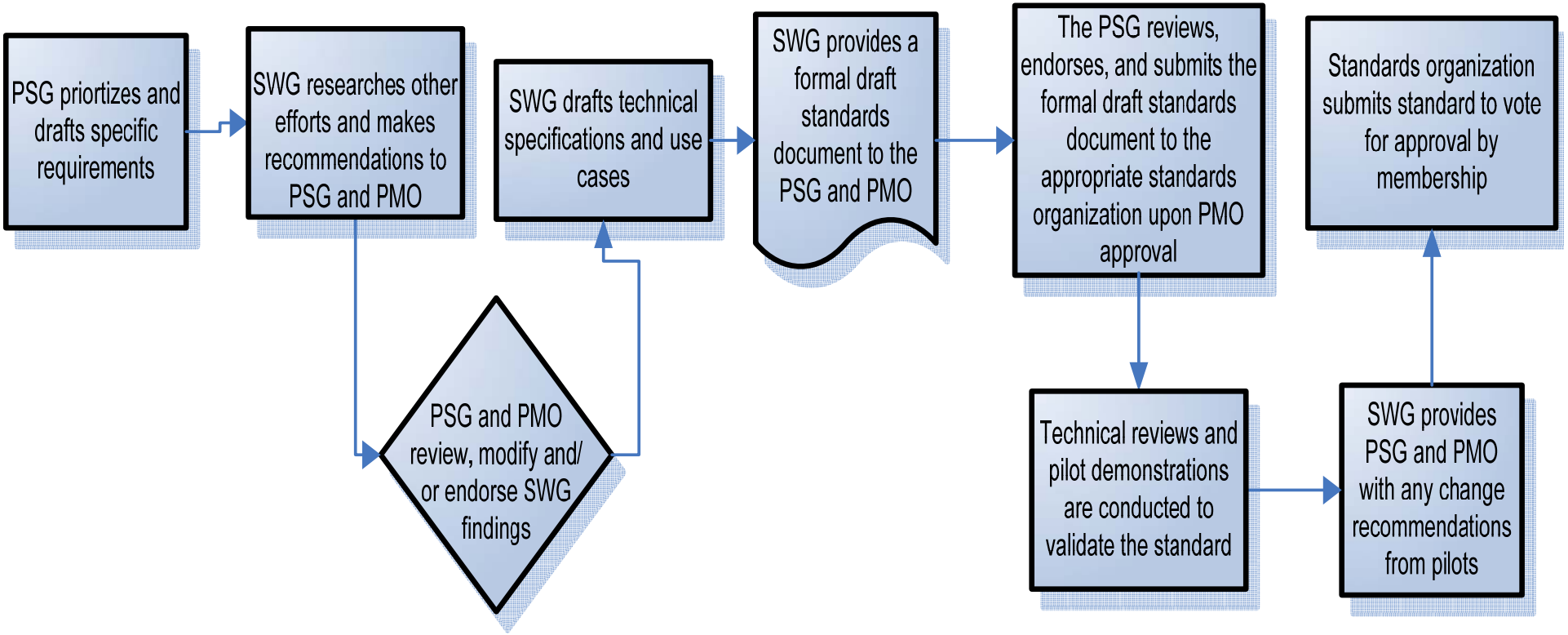
Homeland Security

Value of EDXL Messaging Standards

- Enable efficient preparedness and response and minimize loss of life and property
- Exchange emergency information in a clear, functional context
- Bridge gap between different software products
  - Information sharing between diverse and proprietary systems
- Reduce voice communication redundancies and dependencies
- Open, free, and published standards
- Enable one-to-many communications
- Focus each standard on specific mission tasks and processes

Homeland Security

Standards Development Process



Homeland Security

Partnerships to Develop Standards

The acceleration of standards is a key component of DM's work. DM focuses on messaging and information-sharing standards.

- DM leads the Information Exchange Standards Initiative, a public-private partnership to create messaging standards to share information between disparate incident management systems and software applications.
- DM participates in the National Information Exchange Model (NIEM), which allows local, tribal, state, and Federal governments to effectively share critical information in emergencies, and supports the day-to-day operations of agencies nationwide.

Homeland Security

Key Players in Standards Development

Internal

- U.S. Department of Homeland Security
  - DM practitioner groups including the PSG and SWG

External

- NIEM
- U. S. Department of Justice
- National Incident Management System Integration Center
- Organization for the Advancement of Structured Information Systems (OASIS)
- Emergency Interoperability Consortium
  - Private business community
- National Capital Region Federal Emergency Management Agency Mutual Aid

Homeland Security

Status of Data Messaging Standards

- **Distribution Element (DE)**: DE 1.0 was adopted as a standard in April 2006. DE provides flexible message-distribution framework for emergency information systems data sharing. Messages may be distributed by specific recipients, by a geographic area, or by other codes such as agency type (police, fire, etc.)
- **Hospital AVailability Exchange (HAVE)**: HAVE was submitted to OASIS in January 2006. HAVE provides standard exchange of hospital status, capacity, and resource availability between medical and health organizations and emergency information systems.
- **Resource Messaging (RM)**: RM was submitted to OASIS in January 2006 Jan. 2006 and NIEM 0.21; it supports pilot for National Capital Region Data Exchange Hub. RM provides standard exchange of resource information (persons or things) needed to support emergency and incident preparedness, response, and recovery.

Homeland Security

Common Alerting Protocol (CAP)V1.1

- CAP v1.1 was adopted as a standard on October 1, 2005.
- CAP provides the ability to exchange all-hazard emergency alerts, notifications, and public warnings, which can be disseminated simultaneously over many different warning systems (e.g., computer systems, wireless, alarms, TV, radio).
  - CAP allows for increased warning effectiveness while simplifying the warning task.
- CAP provides a template for effective warning messages.
- CAP is based on best practices identified in academic research and real-world experience.

Homeland Security

US Federal Agency Usage of CAP

- **National Oceanic Atmospheric Administration (NOAA) HazCollect**
  - Local emergency managers can input non-weather emergency messages via CAP for dissemination with NOAA Weather Radio.
  - Reduce alerting time from 7 minutes to 2 minutes
- **Department of Health and human Services – Center for Disease Control (CDC)**
  - CDC Public Health Information Network requires CAP Support
- **Department of the Interior (DOI) – U.S. Geological Survey**
  - Generating CAP notifications on seismic activity greater than 5.0 and volcanic activity
  - Largest user of CAP alerts
- **DOJ**
  - Intra-agency interoperable communications for joint law enforcement activities
- **National Aeronautics and Space Administration**
  - Using CAP to share intelligence between systems
- **DHS Homeland Security Operations Center (HSOC)**
  - Using CAP and EDXL

Homeland Security

Homeland Security