Command, Control and Interoperability

Dr. David Boyd
Director
Command, Control and Interoperability
Science and Technology Directorate
U.S. Department of Homeland Security
January 28, 2009

Homeland Security

Command, Control and Interoperability

Mission

Through a practitioner-driven approach, the Command, Control and Interoperability Division (CID) creates and deploys information resources to enable seamless and secure interactions among homeland security stakeholders.




Vision

Stakeholders have comprehensive, real-time, and relevant information to create and maintain a secure and safe Nation.

Homeland Security

Communications Challenge on the Frontlines

Emergency responders—police officers, fire personnel, and emergency medical services (EMS)—need to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies.

Responders often cannot talk to some parts of their own agencies—let alone across cities, counties, and states. Ineffective communications risk the lives of responders in the field and can mean the difference between life and death for those awaiting help.

Homeland Security

Command, Control and Interoperability

Information

Identify

Communicate

Manage

Visualize

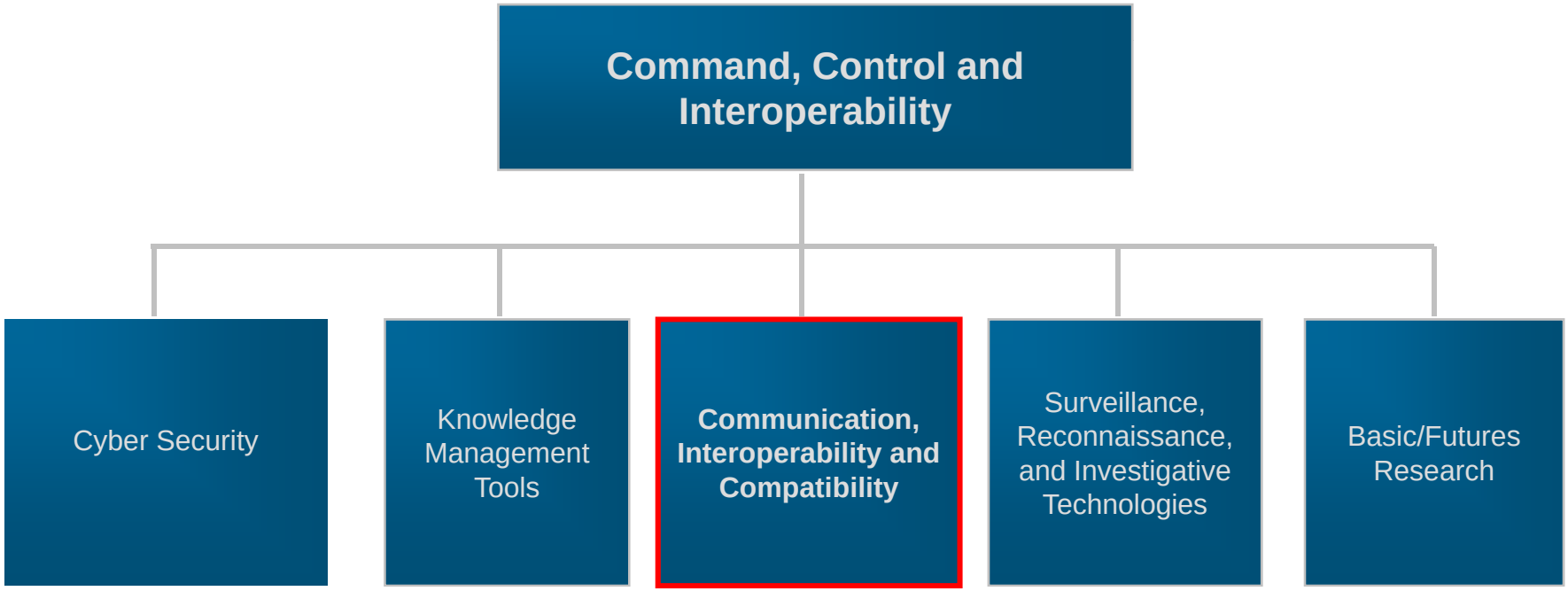
Analyze

Protect

Homeland Security

Command, Control and Interoperability

Through a practitioner-driven approach, the Command, Control and Interoperability Division creates and deploys information resources to enable seamless and secure interactions among homeland security stakeholders. With its Federal partners, the Division is working to strengthen communications interoperability, improve Internet security and integrity, and accelerate the development of automated capabilities to help identify potential national threats.



Why Interoperability Fails

- Locals have almost all the information
- State and Federal agencies need it
- State and Federal direct structures that feed their needs
- State and Federal usually offer litte or no value added or incentive to locals
- So, sovereign locals don’t play
- ***And they rarely need to***

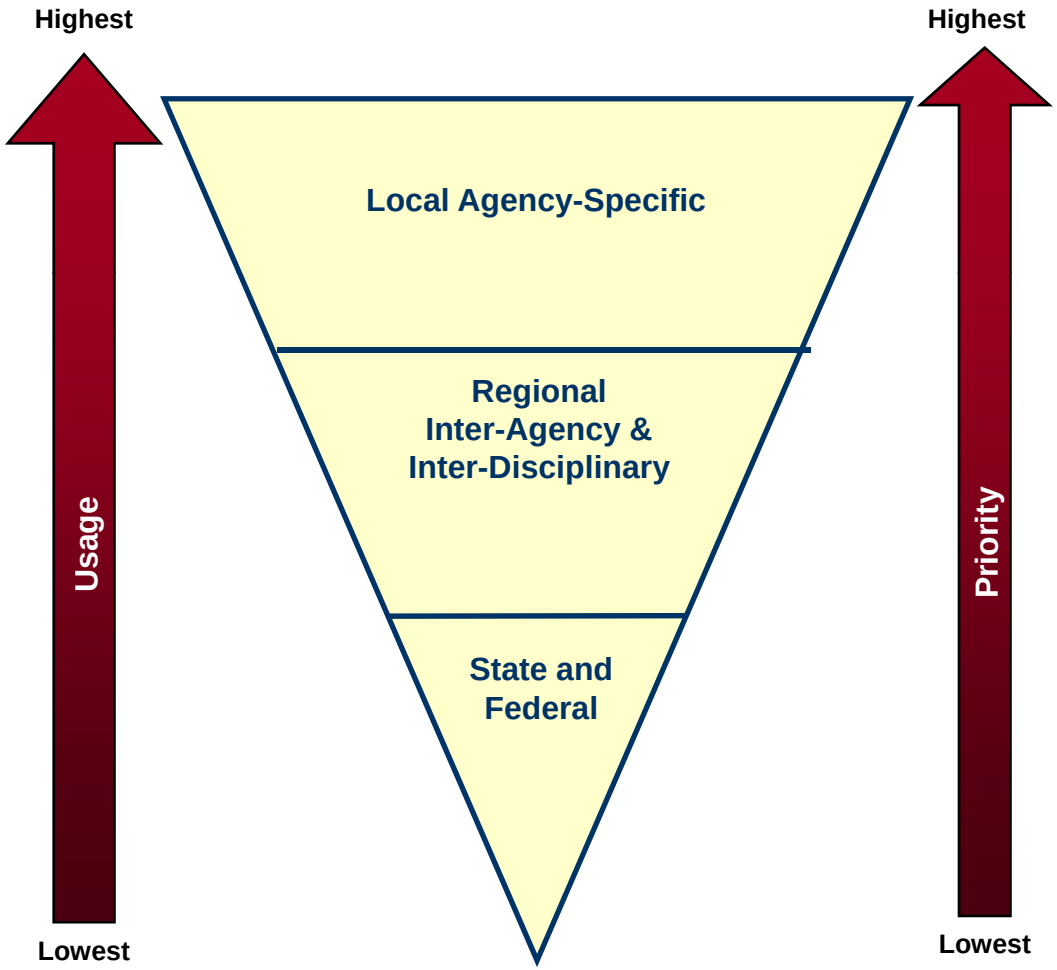
Practitioner-Driven Approach

- A successful strategy for improving interoperability and information sharing must be based on user needs and driven from the bottom up.

- OIC advocates a unique, practitioner-driven governance structure.

- The approach benefits from the critical input of the emergency response community and from local, tribal, state, and Federal policy makers and leaders.

- The approach ensures that resources are aligned with user needs.



Homeland Security

Locals Know

- They have most of the biometric information (fingerprints, etc.)
- Most criminals are local, so they search outward
- More than 95% reside within the state
- Nearly all the rest in adjacent states
- Federal data bases are often last – if at all
- So the key is to incentivize locals – we need them more than they need us

Current Initiatives

Systems Management

Interoperability of Systems

Open Platforms for Emergency Networks (OPEN):

• A supporting infrastructure that allows emergency managers to share incident information regardless of system when using standards-compliant products.

Managing Day-To-Day Information

National Information Exchange Model (NIEM):

• An updated Emergency Management (EM) Domain that allows OIC and NIEM to provide emergency response practitioners with the latest data exchange capabilities for emergency operations. OIC is integrating the Common Alerting Protocol (CAP) and the Emergency Data Exchange Language (EDXL) Distribution Element (DE) data messaging standards into the NIEM EM domain in order to reduce the time and resources required for practitioners to exchange information.

Homeland Security

Acceleration of Standards

The acceleration of standards is a key component of both data and voice interoperability.

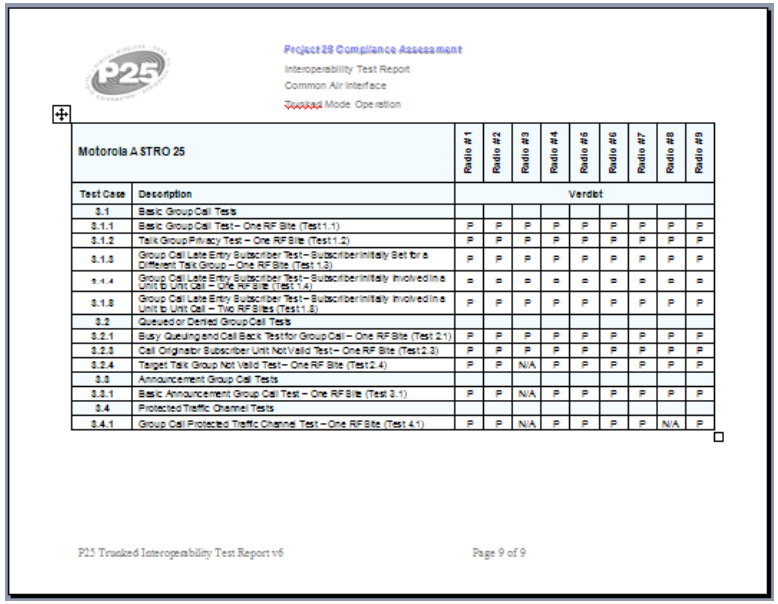
- **OIC supports the acceleration of Project 25 (P25) standards that produce equipment that is interoperable and compatible regardless of the manufacturer. P25 is a suite of eight standards intended to help produce interoperable and compatible equipment.**
- **At the request of Congress, OIC is working with ITS, NIST, the Department of Justice, and the P25 Steering Committee to develop and implement a Compliance Assessment Program (CAP). The Program will validate that P25-standardized systems are P25-compliant and that equipment from different manufacturers can interoperate.**
- **OIC also 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.**

Homeland Security

Project 25 Compliance Assessment

- **Labs are assessed by independent parties prior to being recognized for participation by DHS.**
- **Labs assess/validate equipment as being P25-compliant.**
- **Upon validation, manufacturers declare equipment P25-compliant and submit a Summary Test Report reflecting test results.**
- **An independent Governing Board (GB) represents the collective interests of buyers, sets Program policies, and assists in the administration of P25 CAP.**

Summary Test Report



Project 25 Compliance Assessment
Interoperability Test Report
Common Air Interface
Trunked Mode Operation

Motorola ASTRO 25		Radio #1	Radio #2	Radio #3	Radio #4	Radio #5	Radio #6	Radio #7	Radio #8	Radio #9
Test Case	Description	Verdict								
3.1	Basic Group Call Tests									
3.1.1	Basic Group Call Test – One RF Site (Test 1.1)	P	P	P	P	P	P	P	P	P
3.1.2	Talk Group Privacy Test – One RF Site (Test 1.2)	P	P	P	P	P	P	P	P	P
3.1.3	Group Call Late Entry Subscriber Test – Subscriber Initially Set for a Different Talk Group – One RF Site (Test 1.3)	P	P	P	P	P	P	P	P	P
3.1.4	Group Call Late Entry Subscriber Test – Subscriber Initially Involved in a Unit to Unit Call – One RF Site (Test 1.4)	P	P	P	P	P	P	P	P	P
3.1.5	Group Call Late Entry Subscriber Test – Subscriber Initially Involved in a Unit to Unit Call – Two RF Sites (Test 1.5)	P	P	P	P	P	P	P	P	P
3.2	Queued or Denied Group Call Tests									
3.2.1	Busy Queuing and Call Back Test for Group Call – One RF Site (Test 2.1)	P	P	P	P	P	P	P	P	P
3.2.3	Call Originator Subscriber Unit Not Valid Test – One RF Site (Test 2.3)	P	P	P	P	P	P	P	P	P
3.2.4	Target Talk Group Not Valid Test – One RF Site (Test 2.4)	P	P	N/A	P	P	P	P	P	P
3.3	Announcement Group Call Tests									
3.3.1	Basic Announcement Group Call Test – One RF Site (Test 3.1)	P	P	N/A	P	P	P	P	P	P
3.4	Protected Traffic Channel Tests									
3.4.1	Group Call Protected Traffic Channel Test – One RF Site (Test 4.1)	P	P	N/A	P	P	P	P	N/A	P

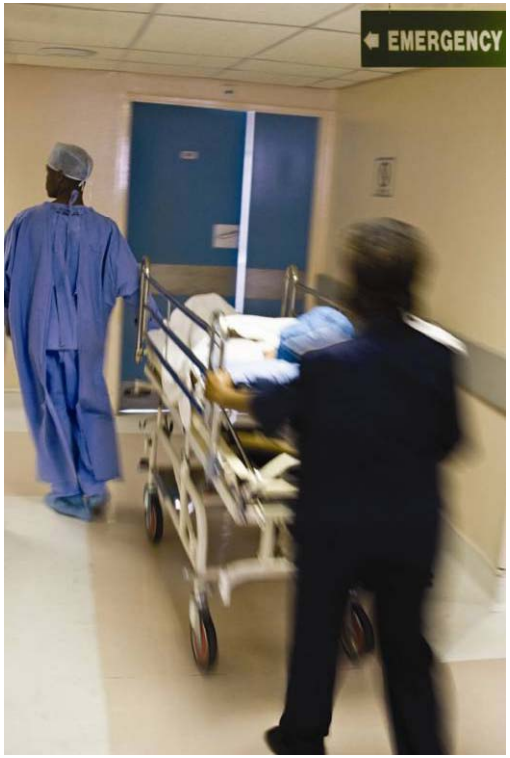
P25 Trunked Interoperability Test Report v6 Page 9 of 9

Provides 'at-a-glance' summary reviews of test results

Data Messaging Standards

- **Data messaging standards enable emergency responders to share critical data—such as a map, a situational report, or an alert—seamlessly across disparate software applications, devices, and systems.**

- **OIC is supporting the development and implementation of the following data messaging standards:**
  - **Common Alerting Protocol Standard**
  - **Distribution Element Standard**
  - **Hospital Availability Exchange Standards**
  - **Resource Messaging Standards**
  - **Situational Reporting Standard**



Homeland Security

Data Messaging Standards

- **Hospital Availability Exchange Standards (HAVE)**

  EDXL-HAVE standard enables responders to exchange information about a hospital's capacity and bed availability with medical and health organizations and others.

- **Resource Messaging Standards (RM)**

  EDXL-RM standard enables responders to exchange resource data for operations, including emergency response personnel and equipment. This information sharing standard will improve emergency preparedness, response, and recovery efforts.

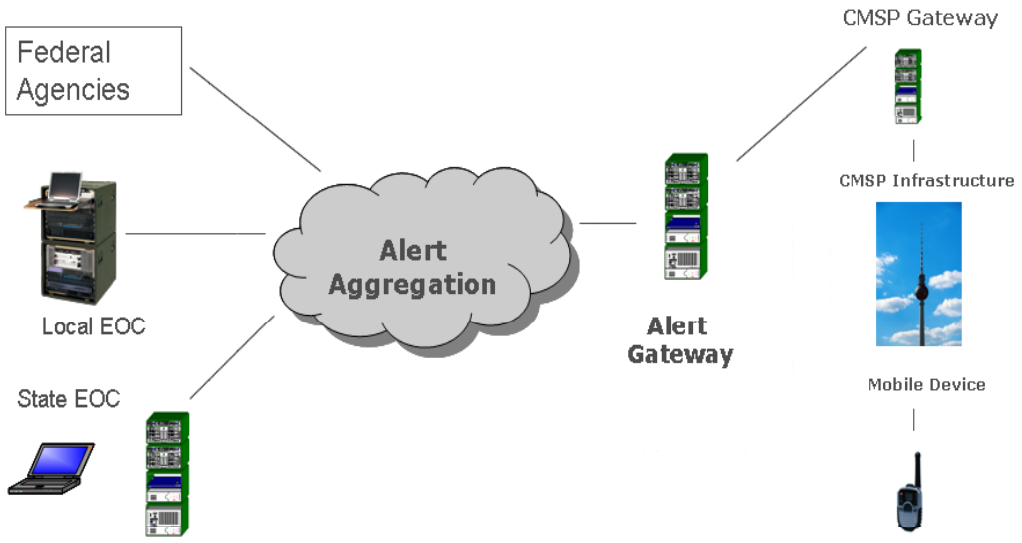
Homeland Security

Commercial Mobile Alert Service (CMAS)

- The **Warning, Alert, and Response Network** (**WARN**) **Act** of 2006 established the **Commercial Mobile Alert Service** (CMAS) to provide emergency alerts to mobile devices. Since over **80 percent of the American population** subscribes to wireless service, this represents significant progress toward a more comprehensive capability to alert people of threats where they are.
- CID owns the **Research, development, testing, and evaluation** (RDT&E) portion of CMAS. Using recommendations from subject matter expertise pooled by the FCC as a starting point, CID's program supports partners to **leverage current technologies while influencing future technologies** in order to increase the number of commercial mobile service devices that can receive emergency alerts.

Major challenges addressed by CMAS:

- **Relevance** of alert based on geographic **location**, **imminence** of threat, native **language**, and **accessibility** of information.
- **Authenticated** origination of alerts that are **meaningful**, **integrated** into a **secure** National infrastructure, and delivered in a **timely** fashion.
- Social science aspects of the **public response** to alerts received on mobile devices, including **public education** and **network use.**



Homeland Security

CIIMS

- **The Critical Infrastructure Inspection Management System (CIIMS) is a new aerial technology that will enable police flight crews to more efficiently manage inspections of important structures such as dams, bridges, large industrial complexes, and urban areas.**

- **A cost effective technology—the hardware package has a current price tag of $3,000—CIIMS enables aviation crews to complete aerial inspections more quickly and efficiently.**

- **For each site, the CIIMS computer uses photographs, geographic coordinates, and inspection questions intended to address the location's security. Flight crews use the system to inspect the site and forward observations to homeland security partners on the ground.**

- **CID is piloting CIIMS in partnership with the Maryland State Police and Los Angeles Police Department.**

- **Readily transferable, CIIMS can assist other state and Federal agencies in their efforts to secure critical infrastructures and resources nationwide.**

Homeland Security

Slide 16

J1 I just edited the slide to reflect new partnership with LAPD also. (added lapd to 4th bullet, took out state police, added 'urban areas' to first bullet)

Jayme.McKinley, 10/6/2008

Homeland Security