



# DMIS/OPEN SIG Presentation

January 7, 2009



Homeland  
Security



# Agenda

- Welcome Message (Avagene)
- Problem Statement (Gary)
- Review approach for federated extensible framework (Gary)
- Presentation of technical CONOPS (Neil and Gary)
- Review of Phased Approach and Timeline for Phase 1 IOC (Sarah)
- Review of IOC Capabilities (Neil and Gary)
- Open discussion and presentation of ways to contribute and provide feedback



**Homeland  
Security**



# Welcome Message

- The Disaster Management Program is proud of our relationship with DMIS and OPEN stakeholders because we rely on input and requirements specified by those who work in or with the emergency management community. We want this dialogue to continue as we discuss our topic today. Please note, we are here to discuss a concept or vision for a potential way to go forward after a very difficult two years. We are counting on your questions and comments just as we have in the past.



**Homeland  
Security**



# Introduction of SIG Topic

- Introduction of topic for SIG
  - Today we will hear about a proposed approach for an open, non-proprietary and extensible, scalable or expandable framework envisioned to provide emergency managers, disaster management related organizations and vendors with enterprise-wide reach and interoperability for existing systems. As visualized, the framework would serve as a preferred point of entry to disaster management information technology systems and a process and common operating environment that can provide the basis for development of an IT R&D roadmap for disaster management. The framework offered for your consideration would promote greater coordination and collaboration between emergency management organizations and vendors, and maximize the value of existing and new systems used to share critical information in times of emergencies. We encourage your participation and questions today. Your comments, suggestions, and feedback are essential to ensure the DM Program moves forward in a manner that meets your needs.”



**Homeland  
Security**



# Welcome Message

- Introduction of speakers – Today we will hear from several speakers.
  - Sarah Hyder, Program Manager, Disaster Management Program
  - Gary Ham, Systems Architect, Disaster Management Program
  - Neil Bourgeois, Systems Development Lead, Disaster Management Program Development Team



**Homeland  
Security**



# Defining the Problem

- Section 214 of the E-Government Act of 2002 called on the Office of Management and Budget, in consultation with the Federal Emergency Management Agency (FEMA), to conduct a study on using information technology to enhance crisis preparedness, response, and consequence management of natural and manmade disasters. The final report from the National Research Council's Committee on Using Information Technology (IT) to Enhance Disaster Management provides ten recommendations for enhancing disaster management through the use of IT.
- The proposed framework that we will review during the presentation specifically addresses four of the recommendations that the report provided. Next we will review each of the four recommendations.



**Homeland  
Security**



# Defining the Problem

- Recommendation 3: The federal government should develop and regularly update an IT R&D roadmap for disaster management with the involvement of a full range of stakeholders.
  - The report highlights the point that disaster management is a system-level problem and that there is not one system out there that satisfies the requirements of all organizations. Dramatic improvements in one technology area may have relatively little overall impact unless other interconnected technologies are able to leverage and utilize the improvements.
  - The report states that a clear vision of end-user goals, a detailed understanding of the individual pieces of the problem and their interrelationships, a detailed understanding of the required technologies, and defined paths for progress would help greatly to inform investment decisions.



**Homeland  
Security**



# Defining the Problem

- The report further states that a number of stakeholders, including first responders, public safety and emergency management agencies, government officials, medical providers, volunteer organizations, infrastructure and transportation system owners, vendors, IT researchers, and disaster researchers, have important perspectives on how to build on existing organizations and technology where possible and how to drive the creation of new, cost-effective technologies and organizational structures where needed. However, an institutional home is needed to launch and sustain such activity.
- Recommendation 4: Federal, state, and local agencies should embrace a diversified acquisition strategy that includes increased use of commercial information technology and greater use of open source software and open standards development as a complement to more traditional acquisition approaches. The report listed a number of challenges that organizations face in adopting IT.



**Homeland  
Security**



# Defining the Problem

- Disaster management organizations often lack the resources to acquire valuable capabilities.
- The development and deployment of many promising technologies are risky and costly given the limited opportunities presented by commercial markets for these technologies.
- In most organizations with disaster management responsibilities, there is no person or unit specifically charged with tracking IT, identifying promising technologies, integrating them into operations, interacting with IT vendors to make sure needs are addressed.
- Decisions regarding IT tend to be made independently by local organizations that must work together in disasters.
- Disaster management is concerned with environments that are intrinsically uncertain and unstable.
- Important sources of funds are typically only available once a disaster has been declared and also must be spent in a short time window.



**Homeland  
Security**



# Defining the Problem

- Recommendation 5: Disaster management organizations should work closely with technology providers to define, shape, and integrate new technologies as a coherent part of their overall IT system.
  - The report points out that reliance on turn-key systems has meant that disaster management organizations have paid less attention to the underlying design issues that ultimately affect the functionality of their IT systems. Often technologies have been acquired as stand-alone products with little consideration for how they integrate with other technologies already in use, even within their own organizations.
- Recommendation 6: In the design, acquisition, and operation of IT systems, disaster management organizations should emphasize the incorporation of disaster response capabilities into the systems that support routine operations.



**Homeland  
Security**



# Defining the Problem

- The report points out that unless experience is gained through routine use or regular training, the full benefits of investment in IT systems are unlikely to be realized. Moreover it is through routine use that the competence and confidence required to successfully use a technological capability, especially in the high-stress situation of disasters, are best developed. However, training large numbers of people to deal with infrequent events poses logistical challenges and is costly.



**Homeland  
Security**



# Key Framework Concepts

- Provides federated platform – Federated is defined as causing to join into a union or league. The framework that we are proposing will provide a platform that will allow for the loose coupling of different systems. This will allow organizations to leverage existing solutions side-by-side and add additional products that can supplement and/or compliment their current systems.
- Provide enterprise-wide reach – Regardless of the Incident Management System (IMS) being used by an organization, the proposed framework will address gaps such as a lack of enterprise-wide reach. The proposed platform will allow existing systems to have an enterprise reach via the federated platform.



**Homeland  
Security**



# Key Framework Concepts

- Framework is entirely web based
- Service component - Each IT system that plugs into the framework will be defined as a service component regardless of whether it serves a single purpose or is a full blown Incident Management System (IMS)



**Homeland  
Security**



# Key Benefits of Framework

- Provides a building block solution that allows multiple products to be combined to build a disaster management system that meets all of an organization's requirements.
- Provides a unified point for maintaining a disaster management focused R&D roadmap.
- Relieves organizations from the burden of having to sift through the myriad of products trying to find a mix of products that will meet their requirements without creating interoperability issues.
- Provides a platform on which vendors can show their unique capabilities and demonstrate interoperability at the same time. Allows an active and effective market to be built.



**Homeland  
Security**



# Key Benefits of Framework

- Promote community-driven development and adherence to standards.
- Promote development of tools for everyday use that can be deployed within the framework.
- Exploit redundancy and diversity to achieve resilience.
- Promote design of systems with flexibility, composability, and interoperability as core guiding principles.



**Homeland  
Security**



# Framework Analogy (iPhone)



- The iPhone provides a framework that allows users to create a computing and communication device that meets their individual requirements.
- The iPhone framework defines ways by which applications can be plugged into the framework.
- The functionality of the iPhone can be extended by adding additional applications.
- The iPhone App store provides vendors with a platform for making their applications available for users to purchase and install within their iPhone framework.



**Homeland  
Security**



# Framework Analogy (iPhone)



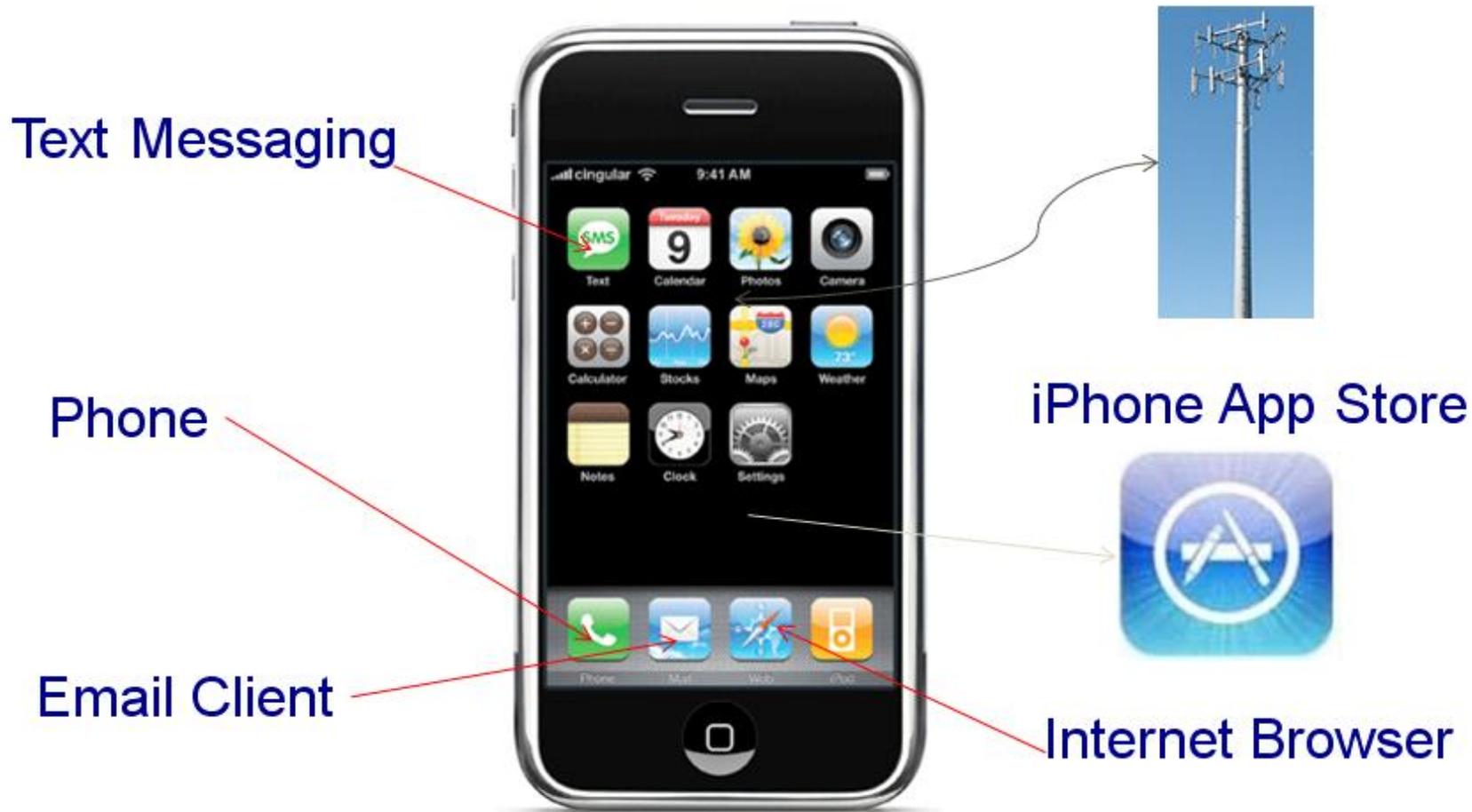
- Each application that is plugged into the framework can take advantage of common framework features as well as obtain connectivity to outside systems via a network connection either through WiFi or Cellular access.
- In many ways the iPhone framework parallels the concept that we are proposing for the federated disaster management framework.



**Homeland  
Security**



# Framework Analogy (iPhone)

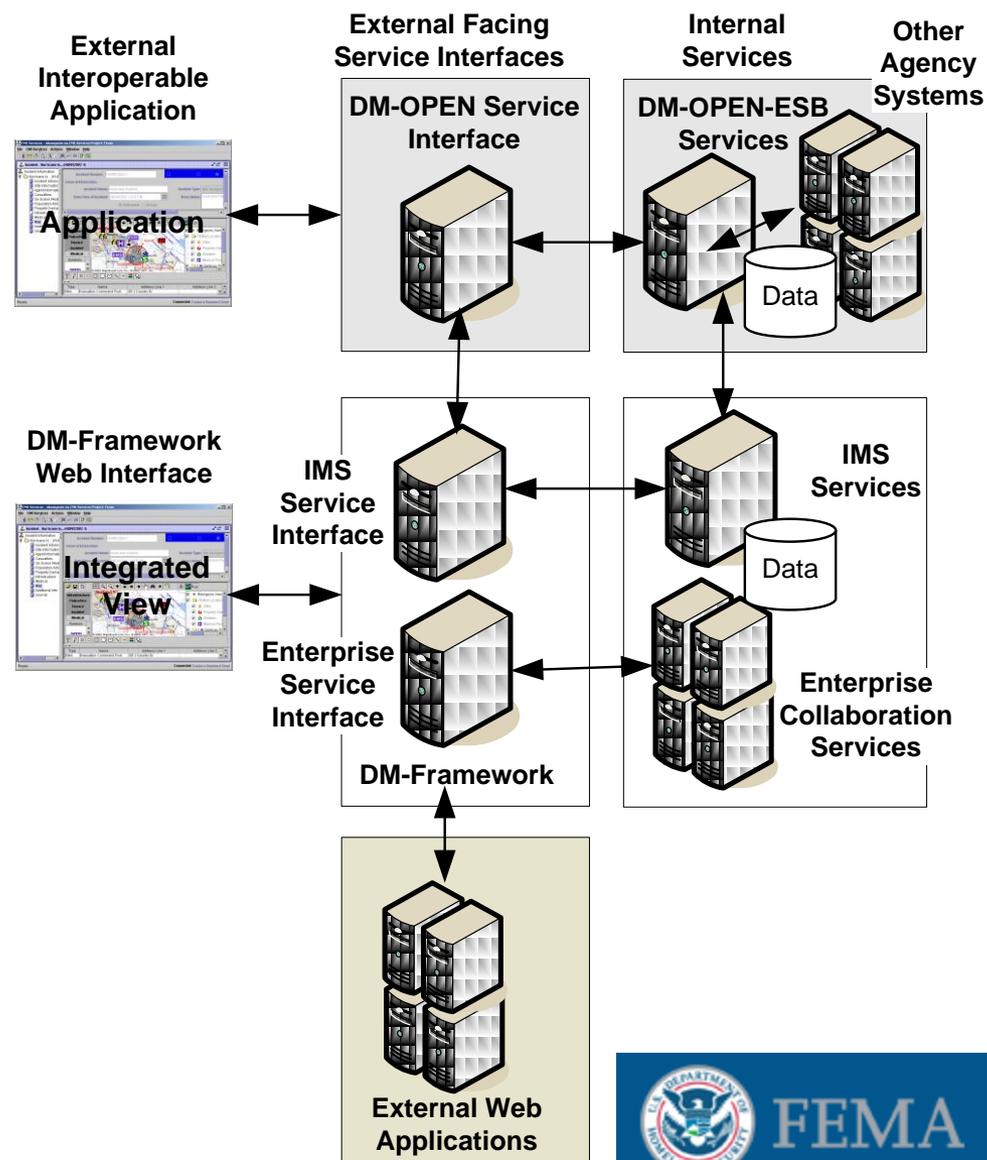


Homeland Security



# DM Framework & OPEN Info Sharing Environment

- The diagram is organized into three high-level vertical tiers from end-user to back end services.
- The diagram is also organized around the following three horizontal swim-lanes which can be separately hosted and loosely coupled.
- This represents an unconstrained view to show the capability that could be incrementally implemented over time.

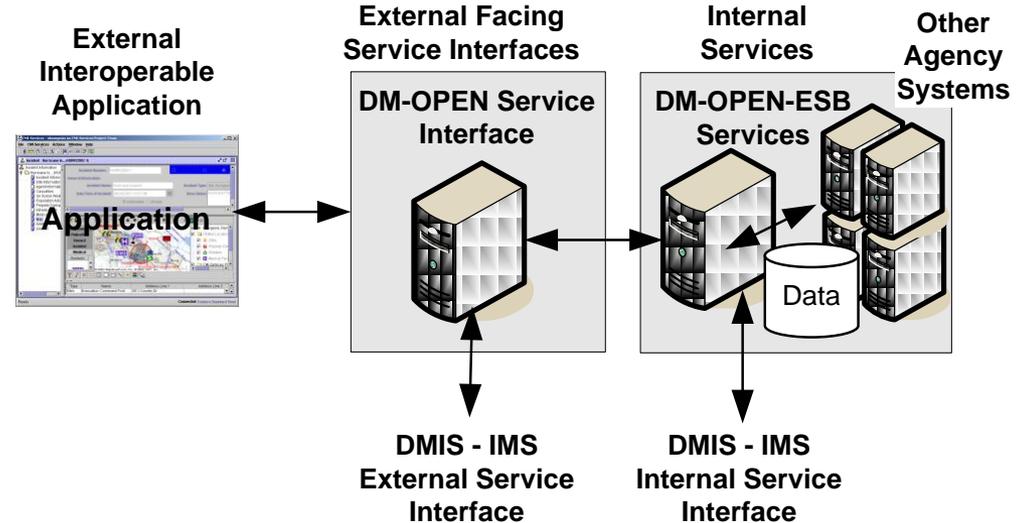


Homeland  
Security



# DM-OPEN Layer

- **External Interoperable Applications** – Utilizes standard-based Web-Services to establish interfaces to DM-OPEN
- **External Facing Service Interface** – Provides the entry point for all external interoperable system interactions.
- **Internal Services** – Exposes services to the DM-OPEN Service Interface and back to external systems via Web-Services. This internal platform can also communicate internally to other agency systems via Web-Services or other data and application interfaces.



Homeland  
Security



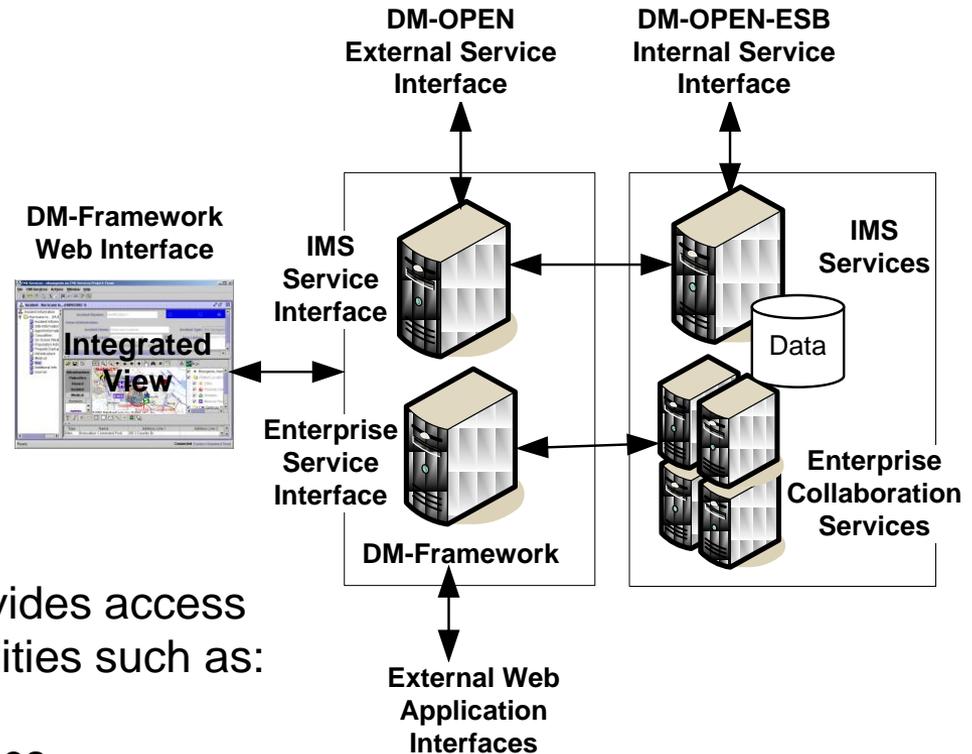
# DM-Framework Layer

- **DM-Framework** – Operators interact via a browser and service interface hosted by the Framework Web-Application.

- **IMS-Service Interface** – Provides access external or DM-Framework hosted COTS/GOTS IMS products configured to operate on the DM-Framework platform portlets.

- **Enterprise Service Interface** – Provides access to potentially a wide range of capabilities such as:

- Single Sign-on
- WMS Interfaces to GIS Repositories
- Interfaces to other external Web-applications and DM-OPEN-ESB platform
- Real Time Collaboration / Data Sharing -> Document Management, Communities of Interest, Instant Messaging, Presence Awareness, Web Conferencing
- Email and Application Integration
- Personalization and Web-Content Management
- Social Networking (DM Community)

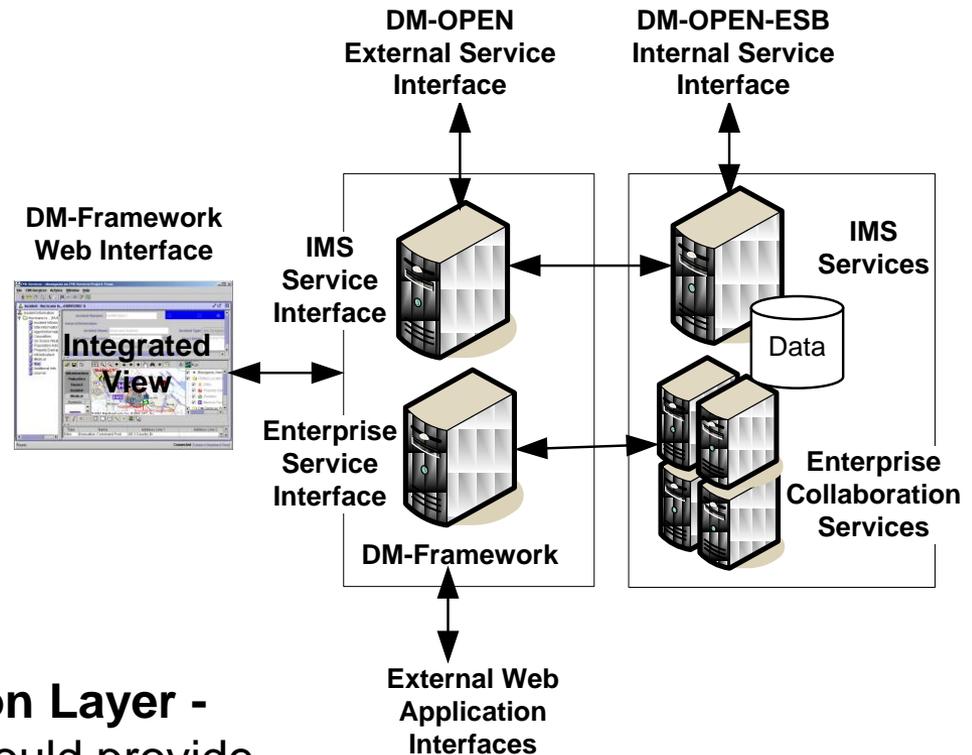


Homeland  
Security



# DM-Framework Layer (Continued)

- **DM-OPEN External Service Interface** – Standards-based Web-Service interface to DM-OPEN.
- **Internal Services** – These include services that support delivery of IMS and enterprise-level functionality as well as communications to internal DM-OPEN-ESB and other agency Services.
- **Interface to External Web-Application Layer** - Enterprise Service Interface Portlets could provide access to other Web-Applications external to the DM-Framework such as:
  - WMS Mapping Services
  - Weather Forecast Services
  - Other local resources important for incident management by a specific Collaborative Operating Group (COG).



Homeland  
Security



# CONOPS Future Example

## (Real-Time/Historical, Incident/Alert Trend Analysis)

- An Enterprise Service Interface could be hosted using an existing COTS/GOTS Web-Application that displays all active and/or historical incidents and alerts plotted to a world-wide map.
  - Data could be retrieved from alerts and situational reports submitted via DM-OPEN along with supporting information provided from other agency systems via Internal DM-OPEN-ESB Service adapters.
  - Incidents and alerts could be represented by icons based on type and status for quicker visual appraisal
  - ICON selection could provide drill down to incident alert details.
- Other capabilities could be established to view incident and alert trends (real-time or historical) along with providing situational awareness at an enterprise-level.
- Operators could readily use other collaboration tools such as Web-conferencing to organize on-line interactive sessions to review trends, walk-through reports or discuss incident and alert details.



**Homeland  
Security**



# Framework Implementation

- A phased approach is being proposed for the development and implementation of the framework along with an enhanced version of DM-OPEN that will build on the current capabilities for interoperable communications.
- The first phase of the framework will provide the basic structure in addition to several out of the box adapters to provide the ability for essential core functionality to be plugged into the framework. This phase is being referred to as the Initial Operating Capability (IOC).
- Phase 1 (IOC) is targeted for completion by September 30, 2009.



**Homeland  
Security**



# Framework Implementation

- The DM team has been undertaking a requirements gathering and modeling exercise for the past month. Requirements have been obtained from current systems, previous SIG meetings and other collection mechanisms. At the end of January we will begin providing the list of requirements to the stakeholder community for feedback and prioritization. The final priority order will be used to determine what will be included in Phase 1 (IOC).
- Subsequent phases will incrementally add additional out of the box adapters to include more and more systems and functionality.



**Homeland  
Security**



# DM-OPEN Web Services (IOC)

- CAP 1.1 Alert
- NWEM Alert (NWS HazCollect).
- EDXL-DE (Emergency Data Exchange Language – Distribution Element) Note: All new emergency data messaging standards will be implemented through the EDXL-DE interface. The EDXL-DE interface can also be leveraged to exchange NIEM (National Information Exchange Model) Information Exchange Packages.
- Improved message retrieval capabilities by leveraging category data structures in the EDXL-DE data structure.
- Hosting or providing access to type lists for use in EDXL-DE messages.



**Homeland  
Security**



# DMIS IOC Planned Capabilities

- Incident planning and response
- Shared interactive maps integrated with incident planning and response
- Resource Request and Tracking
- CAP and NWEM (NWS HazCollect) Alerts
- National map for Incidents and Alerts
- Journal Recording
- Secure instant messaging
- Weather forecast data, doppler radar, and alerts



**Homeland  
Security**



# DMIS IOC Capability Alternatives

- Specific choices on how to implement each of the IOC capabilities have not been made. They will probably include one or more of the following:
  - Enhance an existing FEMA or DHS application to support DMIS
  - Acquire and tailor Other Federal Agencies (OFA) GOTS applications to support DMIS
  - Acquire and tailor COTS applications to Support DMIS.
  - Acquire and tailor Open Source applications
- The Framework allows any number of combinations of the above.
- The Framework also allows users to add there own member applications, from full on IMS to single function application.



**Homeland  
Security**



# Questions?



Homeland  
Security

