

EDXL DEMONSTRATION SCRIPT & SCENARIO



Goal:

Use the recently developed XML-based Emergency Data Exchange Language (EDXL) Header to demonstrate the potential for real data interoperability in the national capital region. Use standardized interfaces and message sets to demonstrate how a group of cross-jurisdictional emergency response/government agencies using disparate communications systems can effectively generate, receive and update emergency messages in real-time.

Key characteristics to be demonstrated:

- Allow multiple responders to easily communicate about the same event despite their use of different products and services using the emerging routing method of a common EDXL Header, common to all stakeholders.
- Demonstrate that individual companies/organizations have control over what information they send and what information they receive.
- Demonstrate that government and emergency response agencies will be notified about emergencies that they otherwise would not know about in real time, thus saving time and resources.
- Demonstrate a core emergency data communications architecture using a standards-based, scalable, multi-vendor approach integrating legacy systems with new web-based technologies.
- Demonstrate that standards-based interoperability does not require months of “one-off” preparation. Demonstrate an approach showing it can be done quickly and relatively inexpensively by publishing the standard and interface, and entering into a cooperative agreement.
- Create a replicable demonstration model of interoperability for regional and national use.

Demonstration Overview:

The demonstration will take place at the George Washington University in Washington, DC on October 27th at 10:00 a.m. Multiple agencies from the region encompassing a broad spectrum of the emergency response community from all levels of government will participate. Some agencies will participate using their existing technology. Other agencies will use some newer technologies. Both will be connected during the demonstration.

Introduction

- Introductory remarks welcoming guests (**Frank Cilluffo, Vice President of Homeland Security, GWU**) (5 minutes)
- Brief description of the world today, lack of interoperability and common standards across jurisdictions and disciplines; Direction being taken to solve problem; Explanation of EDXL process and the demonstration of the Header (**Gordon Fullerton, Department of Homeland Security; others**) (20 minutes)
- Begin Demonstration (30 minutes)
 - As demonstration is unfolding, representatives of the local emergency response community will describe the scenario and how the information being shared is beneficial to them

Scenario Overview:

Scenario Step 1:

- DHS raises homeland security threat level to red after obtaining very credible evidence that a plot to hijack commercial trucks and drive them into government buildings in the capital. DHS sends detailed threat information to all emergency response agencies in US.

Technical Interface 1:

- Message is sent using **EPAD Connect (EC)** from DHS to all agencies registered to receive terrorist threat messages. This will include messages to other EC users as well as a direct feed to DMIS where other systems can pull message and a direct feed to other systems registered in EPAD to receive direct feed.
** We will actually show the live creation of the message in the room.

****Throughout the duration of the event we will toggle back and forth between different systems that are receiving messages even though they are not generating them (e.g. EMMA, MyStateUSA, DisasterHelp)**

Scenario Step 2:

- Message is sent from OnStar national call center to a North Carolina County 9-1-1 agency alerting them that a customer believes he witnessed a silver tanker truck with placard number 1017 being stolen by two men at a rest stop in Nash County, NC on I-95 northbound. There was a delay of one and half hours from when potential theft was witnessed and when it was reported.

Technical Interface 2:

- OnStar sends a commercial vehicle theft message to NC County 9-1-1 agency using **EC**.

** We will not show the live creation of this message in the room. It will be done off-site or will be done in the room, but not visible to guests.

Scenario Step 3:

- Commercial vehicle theft message is sent from NC County 9-1-1 agency to all agencies in North Carolina, VA and the DC Metropolitan area who are registered to receive commercial vehicle theft messages. Message indicates truck is carrying chlorine.

Technical Interface 3:

- NC County 9-1-1 agency sends a commercial vehicle theft message using EC. Message is received by EC users as well as a direct feed to DMIS where other systems can pull message and a direct feed to other systems registered in EPAD to receive direct feed.

** We will not show the live creation of this message in the room. It will be done off-site or will be done in the room, but not visible to guests.

Scenario Step 4:

- A commercial fleet company reports to Nashville 9-1-1 agency that a tanker truck with license plate TN-12345 carrying highly flammable methyl ethyl ether headed for Ohio has broken a geo-fence and is now headed towards the capital region on Rt. I-40 east.
- Nashville 9-1-1 agency sends commercial vehicle theft message to all agencies in TN, NC, VA and the capital region.

Technical Interface 4:

- Nashville 9-1-1 agency sends a commercial vehicle theft message using EC. Message is received by EC users as well as a direct feed to DMIS where other systems can pull message and a direct feed to other systems registered in EPAD to receive direct feed.

** We will not show the live creation of this message in the room. It will be done off-site or will be done in the room, but not visible to guests.

Scenario Step 5:

- Due to heightened security level a terrorist threat message is sent from DC Police agency to all agencies in the capital region alerting them that two trucks filled with gasoline and chlorine are potentially headed to DC and it could be part of a terrorist plot. Be on alert.

Technical Interface 5:

- DC Police agency sends a terrorist threat message using **E Team**. Message is stored on DMIS server where it can be pulled into other applications. WebEOC, Blue 292, EMMA, MyStateUSA, SDI, EC, DMIS Tool, DHelp pulls message and delivers it to DHelp users etc. Similarly, EPAD Connect will and E Team may have direct connection to EPAD to send messages directly to other agency applications registered to receive terrorist threat messages (EMMA, Fire Monitoring Technology International).

Scenario Step 6:

- A radiation sensor located at a toll booth at the Ft. McHenry Tunnel just outside of Baltimore on I-95 in Maryland, 40 miles north of DC registers a very high level of radiation, levels high enough to include a potential dirty bomb, after a van drives through the toll. Maryland Transportation agency alerts MD police agency of the radiation alarm. MD police agency alerts all agencies in the capital region of the potential dirty bomb and requests that MD EOC be activated and that their hazmat team be ready for response. MD police agency indicates that they will be setting up a road block on I-95 South before the I-495 Beltway intersection.

Technical Interface 6:

- Maryland police agency sends a terrorist threat message using **DMIS Tool Kit**. Message is stored on DMIS server where it can be pulled into other applications. DHelp pulls message and delivers it to DHelp users, WebEOC, E Team, EMMA, Blue 292, etc. Similarly, EPAD Connect will and E Team may have direct connection to EPAD to send messages directly to other agency applications registered to receive terrorist threat messages (EMMA, Fire Monitoring Technology International).

Scenario Step 7:

- Agency to agency specific needs request message will be sent from MD EOC to VA EOC asking them to activate their hazmat team and be prepared to respond locally in VA or provide assistance in MD.

Technical Interface Step 7:

- Application to application hazmat message will be sent from **Blue 292 to WebEOC**. (done by sending a message from the Blue 292 COG with a limited distribution to the WebEOC COG)

Scenario Step 8:

- Truck heading towards DC with gasoline stopped and criminals apprehended by VA police agency.

Technical Interface Step 8:

- VA police respond to initial commercial vehicle theft message using **Blue 292**. Message is stored on DMIS server where it can be pulled into other applications.

Scenario Step 9:

- Tanker truck from NC is located a few miles outside of DC on I-395 North and is being pursued by VA police agency. Tanker truck veers out of control at the I-395/I-295 intersection in Washington, DC. VA police agency sends a hazmat message to agencies in DC and surrounding counties alerting them of hazmat spill.

Technical Interface Step 9:

- VA police send hazmat message using **E Team**. Message is stored on DMIS server where it can be pulled into other applications.

Scenario Step 10:

- DC fire and rescue agency responds to hazmat message requesting area evacuation within 1 mile radius of spill. DC EOC is activated. Hospital availability in VA is checked since GW Hospital ED is closed. Instructions on how to treat chlorine are sent to responding agencies.

Technical Interface Step 10:

- DC fire and rescue agency responds to hazmat message using **WebEOC**. Message is stored on DMIS server where it can be pulled into other applications.
- Since DC fire and rescue agency knows that nearest hospital in DC (GW Hospital) ED is closed to new patients, it can check hospital availability in VA by viewing info available on VHHA hospital availability website through a link in WebEOC. (We will describe that we are working towards getting the hospital availability messages in EDXL format as well for VHHA, FRED, etc.)
- To demonstrate ability to use information being received and add valuable information to it, SDI will mine data sources for information on how to treat chlorine, and respond to hazmat message with chlorine treatment instructions.

Scenario Step 11:

- Message is received by agencies who have systems capable of alerting public safety and government leaders, as well as the public, by sending targeted messages to cell phones, pagers, PDA's, etc.

Technical Interface Step 11:

- Alerting companies and public dissemination sites ([MyStateUSA](#), [DisasterHelp](#)) parse hazmat message into their systems (via connection to DMIS) and deliver messages to phones, pagers, etc. of participating public safety/government leaders.

Scenario Step 12:

- MD police agency successfully stops the van carrying dirty bomb and apprehends criminals.

Technical Interface Step 12:

- MD police agency update initial hazmat message using [DMIS Tool Kit](#) indicating van has been stopped and call for hazmat team and bomb squad to come to scene to analyze bomb.

Summary Explanation/Importance for Emergency Response (10 min)

- Explanation of general demonstration principles and architecture and specific methods of data sharing that were enabled by using the EDXL Header, and why that is important (**Dr. Jack Potter, Vice Chair, ComCARE Alliance**)

Future Outlook (10 min)

- Discussion of the work that still needs to be done and specific next steps (**Gordon Fullerton, Department of Homeland Security**)

Q & A for Participants (10 min)

Vendor Show and Tell (end of demonstration until 12:30)

- At the close of the demonstration, participating vendors will have ample time to display their individual technologies to participating government and emergency response agencies. Speakers will encourage audience participants to examine the individual technologies being demonstrated.