

WHITE PAPER

This document is currently for concept exploration only and is not to be distributed to the general public.



FEMA

OCIO, Enterprise Architecture Staff

FEMA TAV Program Management Office

FEMA IPAWS Program Management Office



**United
States
Air
Force**



USAF Cyberspace Task Force



**United
States
Coast
Guard**



Coast Guard Innovation Council

Asset Tracking Protocol

Enhancing Interoperation in Emergency Response Between the Department of Homeland Security, the Department of Defense and State and Local Governments

White Paper ☆ Asset Tracking Protocol

Background:

The 911 commission called for a higher degree of interoperability between state and local government. One enabler for such interoperability would be to fill the gap in digital communications standards applicable to the problems at hand. The Department of Homeland Security established a strategic partnership with the OASIS standards body to expedite new standards for emergency operations. This would allow software used by state and local government for emergency operations to talk across jurisdictions and also to talk to software used by the Federal Government.

★The first standard resulting from the partnership was CAP, the Common Alerting Protocol, to alert government and the public that a threat was at hand. CAP has been a marked success.

★An informal addition followed, called Amber XML. Its purpose was to support Amber Alerts as mandated by law.

★A “wrapper” protocol, which acts as a letter to a message, was needed to assure that these various formats would reach their intended audiences in different areas and circumstances. Emergency Data Exchange Language– Distribution Element (EDXL-DE) was created for this purpose.

★A means to request aid and supplies and track their expected delivery was required. Emergency Data Exchange Language– Resource Management (EDXL-RM) was created to fill the gap.

★A key component protocol to track infrastructure was stalled in committee. Without this key protocol computer systems could not exchange information on the position and status of emergency vehicles, staff and supplies.

★Hurricane Katrina underscored the need to interoperate effectively.

★The United States Air Force had a protocol used in nearly 100 widely different applications to communicate the status and location of friendly and enemy assets. This protocol is called “Cursor on Target”.

★A “grass roots” effort among engineers began to unify the EDXL environment with proven USAF “CoT” technology. The merged protocol stack is termed the “Asset Tracking Protocol”.

White Paper ☆ Asset Tracking Protocol

CAD and C2:

State and Local Government use software called Computer Aided Dispatch (CAD) to deploy police, fire, ambulance, and sometimes water, sewer, electric and telephone crews. This software allows call centers filled with dispatchers to operate efficiently and effectively. Computer Aided Dispatch is a billion dollar market, and governments have billions invested in their existing plant. The market is mature, and this software has been improved over two decades to become very effective.

The Department of Defense, the Coast Guard and to a lesser extent other federal agencies rely on a different kind of software called “Command and Control” or C2. This software displays forces and allows commanders to redeploy as the situation requires. C2 software is a billion dollar market, and for three decades this software has been improved to high effectiveness.

You can often tell the background of an official in emergency management by which term they use: “Command and Control” or “Dispatch”. Dispatch software handles issues like call taking and jurisdiction far better than C2 software, but C2 software has had far larger development budgets. C2 software has interoperated as many systems working together for several years, while these functions are new to CAD.

Yet other types of software also play a role. This includes software designed specifically to support Emergency Operations Centers or EOCs. It also includes software for disaster logistics.

Important federal government systems have also been created to automate emergency operations. The Disaster Management Information System or DMIS is designed to foster interoperation and create or receive alerts via the Common Alerting Protocol or CAP. The National Incident Management System or NIMS has been created to provide a free and interoperable software system for incident management. The Homeland Security Information Network or HSIN is designed to allow emergency staff to coordinate.

Systems created by the states in conjunction with the federal government or each other are also important. JRIES is a network of emergency systems in the NYC area. The Port of New York and New Jersey system is designed to enhance port security there, and a similar system at Charleston was constructed in conjunction with the Department of Justice.

Many systems have been created, but they do not coordinate and interoperate.

White Paper ☆ Asset Tracking Protocol

Operations Centers etc.:

Operations centers command or dispatch resources to respond to various circumstances. Some estimates say over 300 operations centers were created in response to 911 alone. Many of the 3033 counties in the USA have dispatch systems and qualify as operations centers. The federal government, especially Department of Defense, has many dozens of operation centers.

Operations centers are only one of several types of network “nodes” which must interoperate in a nationwide system to manage emergencies. Many of these facilities exist and building more indiscriminately is unlikely to help in solving the problem. The main challenge is best characterized as coordination or interoperation.

| Node Types | Description | Number |
|------------------------------------|---|---------------|
| Operations Centers | Command and coordination facilities which oversee emergency operations of various kinds | 2000-5000 |
| Warning Centers | Issues public or classified alerts and warnings about impending events | Hundreds |
| Assets | Both first responder and unmanned assets on the front lines of operations | Thousands |
| Validation Centers | Locations dedicated to technical analysis or information reduction | ~100 |
| Distribution Infrastructure | Means to distribute alerts, warnings, alarms | Hundreds |

White Paper ☆ Asset Tracking Protocol

EDXL-DE Details:

The Emergency Data Exchange Language– Distribution Element is designed to solve an important problem. Many emergency operations occur every day, and the vast majority never achieve national significance. How do you distribute information to the interested parties without disturbing the many busy with other emergencies?

The *publish-subscribe* paradigm is used to solve the problem in EDXL-DE. The publish-subscribe paradigm allows individuals to subscribe to a community of interest and receive all the data relevant to that community. For example a community of interest may be restricted by jurisdiction– say Gotham City. Officers in nearby Jersey City do not receive data about Gotham, which would overwhelm their communications with excess information “noise”.

Jurisdiction is a particularly interesting problem because it is not shared by existing military C2 solutions. Addressing this problem is critical to success in the civilian emergency operations domain.

EDXL-DE also contains a means to subscribe by geographic area. You could potentially subscribe to only one borough of the Gotham City traffic, or one beat in Gotham, by restricting the subscribed area.

Communities of interest also allow operations to be created by crisis. For example, you can create a community for the future Hurricane Mischa crisis. In fact, knowing the names of hurricanes in advance would let you create communities in advance of the actual hurricane.

The paradigm of communities allows distributed opt-in to information. Unlike the military, the civilian world is not organized into a rigid hierarchy. Different organizations make independent decisions. Some, like the American Red Cross, are not even government organizations.

The use of EDXL-DE is critical to success in the civilian domain. Not only is it part of the standards suite that is overwhelmingly accepted as the authoritative specification for emergency operations, but it also provides key capabilities not available or needed in military protocols.

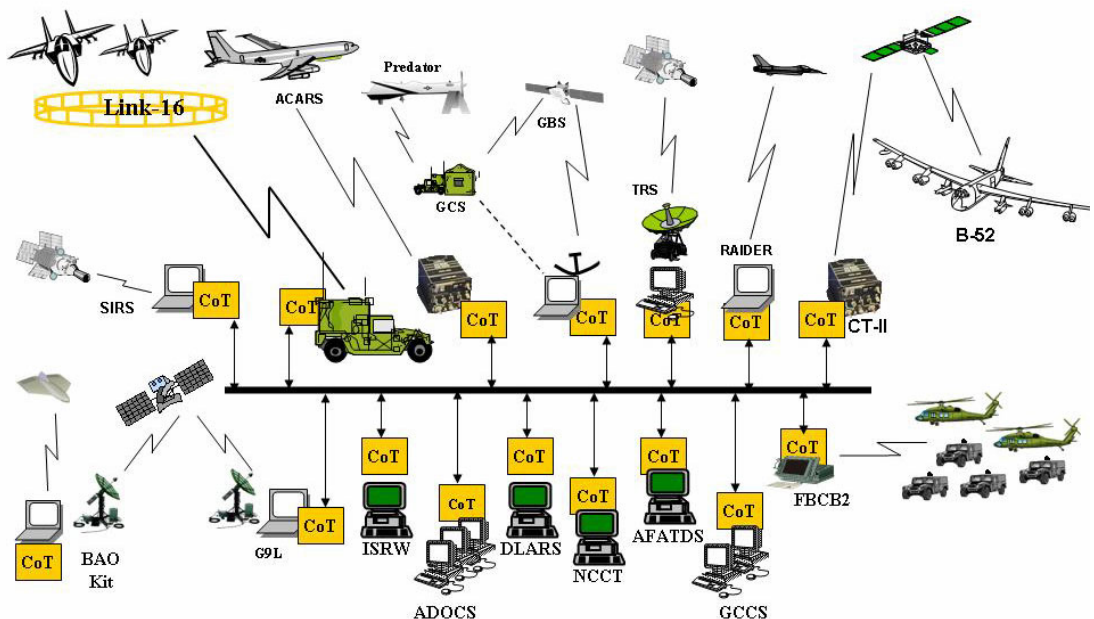
White Paper ☆ Asset Tracking Protocol

Cursor On Target in Detail:

The DoD uses a large number of mission-critical computer applications, and data exchange between them has long been a problem. The need for interoperability was tragically highlighted in blood during a friendly-fire incident in Afghanistan. An accidental transposition of target coordinates resulted in allied aircraft engaging a team of USAF special operating forces. The consequences were unfortunately very lethal. After months of hospitalization, one surviving team member noted that machine-to-machine communications would have averted this loss of life.

The Cursor-on-Target, or CoT, message format was designed to address these integration dilemmas. To date, CoT has been implemented for more than one hundred different systems and has linked the special operating forces to the digital, real-time, information they need to execute their missions.

Cursor-on-Target, or CoT, organizes information in a very simple, hierarchical structure placing the most important pieces of information in the most accessible positions within the message. Common to all CoT messages is information on the “what, where,



when” of the object being described. The CoT format is highly extensible, very stable, and new information can be added easily. This is precisely the type compact, low-overhead messaging needed to update displays of many hundreds or even thousands of objects that move or change status.

The present effort is a natural progression of merging the CoT protocol created in response to a battlefield tragedy, and the OASIS protocol efforts developed in response to 911.

White Paper ☆ Asset Tracking Protocol

Status Codes:

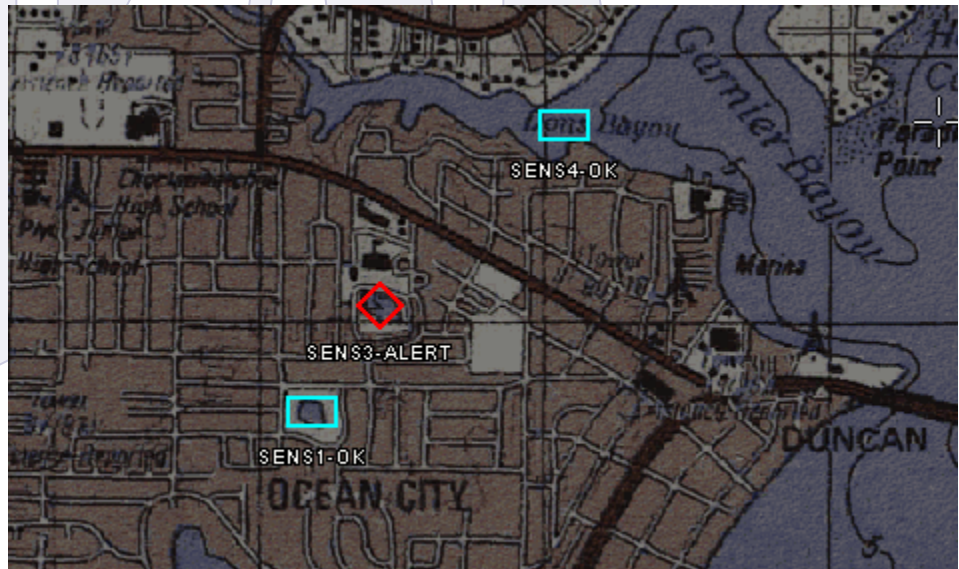
In combination, CoT and EDXL can provide the functions required for asset tracking, but gaps do exist. Specifically, CoT has focused on the integrating military systems and lacks some of the vocabulary needed in civilian data exchanges. In particular, CoT's vocabulary must be extended to include:

- ☆ The "10 codes" used in police, fire, and ambulance status reports.
- ☆ Access control and intrusion detection status for buildings and warehouses monitoring.
- ☆ Status of shipments and containers in the supply chain.
- ☆ CBRNE (Chemical Biological Radiological Nuclear and Explosive) alarm codes and status messages.

Other Issues:

Several other issues need to be addressed as CoT is merged with the OASIS standards.

- ☆ CoT's asset types must be harmonized with EDXL-RM's resource types.
- ☆ CoT will need to express alerts as reported by the Common Alerting Protocol (CAP).
- ☆ CoT message refers to an asset. This reference must be understandable as a resource requested or supplied in EDXL-RM (Resource Management).
- ☆ CoT may need to carry geospatial information as described by an OGC object.



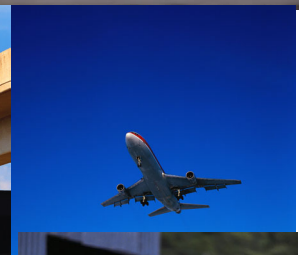
These issues are few in number and not technically challenging, and work to extend CoT for these applications is already underway.

White Paper ☆ Asset Tracking Protocol

Assets:

What do we mean when we say assets?

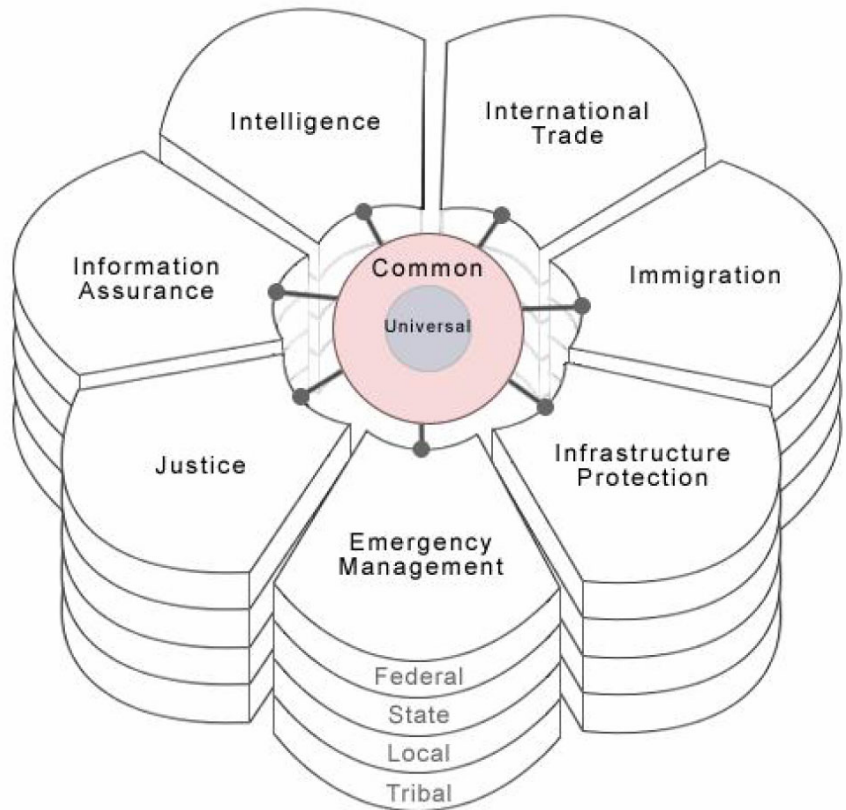
- ★ Federal agents carrying Blackberries or Cell Phones
- ★ State Police
- ★ Municipal Police
- ★ Agent or Police Vehicles
- ★ Helicopters and Aircraft
- ★ Emergency Supplies in Shipping Containers
- ★ Generators
- ★ Buildings
- ★ Access Control Points
- ★ Nuclear Plants
- ★ Chemical Plants
- ★ Emergency Operations Centers
- ★ Badge Readers
- ★ Security Desks
- ★ Radiological Portals
- ★ Surveillance Systems
- ★ Unmanned Aerial vehicles
- ★ Unmanned Underwater Vehicles
- ★ Border Control Points
- ★ Ports
- ★ Cargo Ships
- ★ Cargo Aircraft
- ★ Shipping Containers
- ★ Airborne Shipping Containers
- ★ Refineries
- ★ State Parks
- ★ Statuary
- ★ Elected Leadership
- ★ Ambulances
- ★ Fire Trucks
- ★ Rescue Trucks
- ★ First Responders
- ★ Emergency Cell Phone Restoration Vehicles (SOWS and COWS)
- ★ Busses full of evacuees
- ★ And much more...



White Paper ☆ Asset Tracking Protocol

Governance:

Federal government has the required management structures to manage the introduction and implementation of standards to interoperate with state and local government. Perhaps the most visible and widely known is the National Information Exchange Model or NIEM. NIEM is a joint venture of DOJ and DHS covering the areas shown at right.



The Disaster Management e-gov initiative provides support for OASIS standards, especially the Common Alerting Protocol (CAP) portion of EDXL. They provide free software (DMIS) as a reference implementation. The program also provides a website for information at www.disasterhelp.gov.

Paradoxically the hardest standards adoption process concerns use of the OASIS standards within the Federal Government itself. DHS has an effort at the time of the writing of this document to determine which standards are to be used in the department. DoD has been an enclave of proprietary information formats, but the USAF Cyberspace Task Force seeks to make significant inroads by moving the CoT protocol to use as a public standard.

The Federal Enterprise Architecture efforts at OMB may play a role by placing the OASIS standards within the list of government wide standards for future use. Work is in progress.

Many legacy systems will have to be converted to use the OASIS standards to achieve interoperation with state, local and tribal government. This requires popularization and education of various project managers and vendors managing and providing government systems.

White Paper ☆ Asset Tracking Protocol

Distribution of Messages:

Past Distribution Systems:

In the 1990's various local governments worked to interconnect their dispatch systems in the state of California. The idea was to improve service in an area of high congestion. The system was called INTERCAD.

INTERCAD worked by allowing the several participating governments to use their existing software. That software was a significant capital and operational investment and replacing it was infeasible. A single central system for all the participants was not considered; that would have resulted in lower reliability by introducing a single point of failure and would have decreased throughput. The systems were linked, not replaced.

To do this an EAI (Enterprise Application Integration) server was added. It allowed each system to send messages in their native format. The EAI system translated between them and routed or distributed the correctly reformatted message to each required recipient.

INTERCAD was a success. It has been replicated across the country. Similar systems are being installed today.

A standard format and XML routing:

While systems like INTERCAD work an additional expense and occurs because no standard format is used. If a communications standard were used by the many vendors of dispatch systems no EAI system would have to be purchased and no message translation function would be needed.

After 911 DHS (Department of Homeland Security) teamed with the OASIS standards body. In 2005 many dispatch system vendors participated in an interoperation exercise sponsored by the Executive Office of the President. The OASIS standard suite has expanded to encompass many functions.

A portion of the OASIS standard addresses routing and distribution of messages to all parties who want it and are authorized to receive it. Implementation of that portion of the standard uses XML content based routing and applies new technology to deliver scalability and sophisticated management of messages required for large scale use.

White Paper ☆ Asset Tracking Protocol

Success Factors:

Success in adoption of CoT may be measured by adoption within the following efforts:

- ☆ Incorporation within the OASIS emergency standards.
- ☆ Incorporation of the OASIS emergency standards within the NIEM or National Information Exchange Model.
- ☆ Incorporation of the NIEM and OASIS standards within the DHS list of accepted standards (TRM).
- ☆ Adoption of the NIEM and OASIS standards as the interoperation mechanism between DHS and DoD.
- ☆ Adoption of the EDXL standards, including CoT, by the OMB via FEA (Federal Enterprise Architecture) TRM (Technology Reference Model) on the national level.
- ☆ Creation of a driver for CoT that incorporates EDXL-DE at MITRE.
- ☆ Creation of EDXL routing software that understands CoT payloads.
- ☆ Ability to repackage CoT within EDXL-DE into EDXL-DE within COT (and vice versa) at the boundary for interoperation between the military and civilian infrastructure.

Key Systems & Programs:

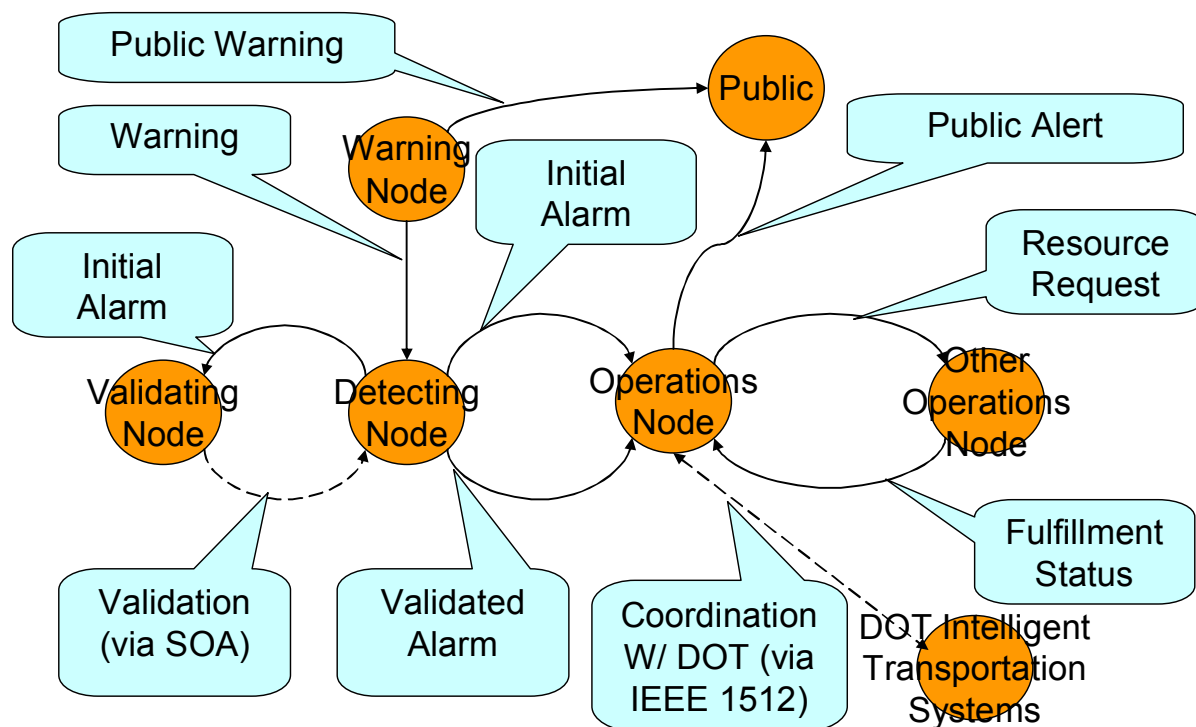
- ☆ NIMS, the National Incident Management System, is the primary system distributed by the Federal Government to manage incidents of all kinds.
- ☆ Homeland Security Information Network is the primary system to be used for messages and collaboration in emergencies and counterterrorism.
- ☆ The Disaster Management Information System is free software sponsored by DHS to promote interoperation in disasters.
- ☆ The Integrated Public Alerts and Warnings System will replace the older and aging warning systems used to distribute nationwide warnings.
- ☆ The Global Nuclear Detection System will combat nuclear terrorism.
- ☆ The adoption by CAD vendors will be critical. Dispatch is a billion dollar business with over 20 vendors in the US.
- ☆ The state of New York, the NYC area and the Washington DC area have important prototype systems for combined operations.
- ☆ The ports of New York and New Jersey and the Port of Charleston have leading edge systems for counterterrorism.

White Paper ☆ Asset Tracking Protocol

Ready Set Go

To understand the broad context in which the asset tracking protocol will be used, think “ready-set-go”. First an alert or warning is issued to watch out for potential disaster: *READY*. Then someone detects that the disaster may be occurring: *SET*. The disaster is verified or validated (to filter out the “cry wolf” effects and false alarms) and then finally the alarm is sounded for action: *GO!*

The standard protocol for *READY* is the Common Alerts and Warnings (CAP) protocol. The *SET* messages are handled by a wide range of technical messages such as ANSI 42.42, OGC SOS and SAS (Open Geospatial Consortium Sensor Alert System and Sensor Observation System), GJXDM (Global Justice XML Data Model), and more, possibly in conjunction with the asset tracking protocol. The *GO* message is transmitted via the asset tracking protocol. Disasters are then managed by protocols like IEEE 1512 for transportation systems and EDXL RM to request resources.



White Paper ☆ Asset Tracking Protocol

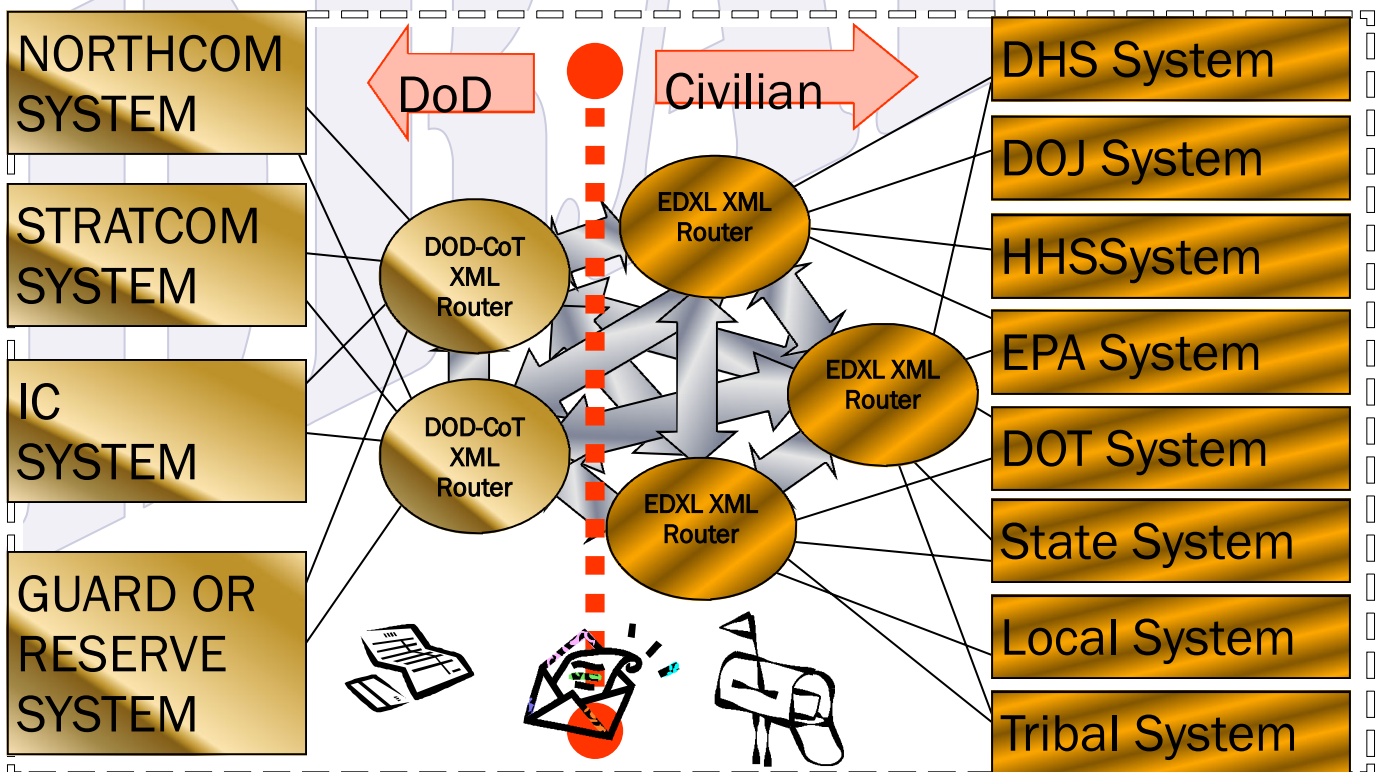
Interoperation with DoD

Department of Defense has a large legacy infrastructure with billions of dollars of investment in proprietary protocols. How can DoD interoperate with the civilian community through the asset protocol stack of CoT in an EDXL wrapper?

A DoD XML router backbone is being built, and so is a civil XML router backbone. The civil routers will move EDXL and other (CAP, Common Alerting Protocol) messages, while the DOD routers will move CoT and other DoD protocols. The civilian routers will manage messages by community and jurisdiction, while DoD will route by subject.

At the border the XML routers will translate message formats for some messages. For CoT the EDXL “envelope” will be added as messages move from DoD to civilian sides, and the envelope of EDXL data will be removed from CoT messages in the other direction.

DoD systems will not need to adopt EDXL protocols directly, and civilian systems need not adopt DoD protocols where public ones exist. This will potentially save billions of dollars.



White Paper ☆ Asset Tracking Protocol

Vision:

A truck containing building materials leaves northern New York state for repairs to levees in the gulf coast. The situation is critical, and if a dam is not repaired with these materials it may break. The route for most of the journey will be I95.

The truck is visible to the NOC (formerly HSOC) using the IRRIS system as it leaves. As the truck nears NYC it is visible to the PNYNJ system and the joint regional EOC. The EOC arranges for a New York state trooper to act as escort, switching off to a New Jersey trooper at the state border.

As the truck nears Washington DC Maryland and Virginia state troopers are enlisted as escorts via the DC regional EOC.

In South Carolina the truck nears SEAHAWK and they note its arrival. While not directly related to the port, SEAHAWK brings the arrival to the attention of the radiological pilot program, and each weigh station. As the truck nears the weigh station call it on CB radio to tell it to pass by.

As the truck nears the disaster area an operator using Eagle Vision to view the latest satellite imagery notes that the highway ahead is jammed and arranges to have a trooper escort the truck on a detour to expedite the delivery.

Meanwhile, on the Mexican border, a smuggler attempts to cross the open desert.

The SBI system notes his crossing. A CBP agent vehicle, on sheriff's vehicle and a helicopter are routed to the scene.

The helicopter has not arrived, but the smuggler has headed for one of two ravines commonly used to avoid interception. Each vehicle, noting the position of the other via PDA, positions itself at the head of a different ravine and waits.

The helicopter flies overhead, directed by the CBP vehicle to the right area via PDA. It flies a search pattern and locates the smuggler. 10 illegal aliens are saved from the sweltering heat in the unventilated truck, and 20 kilos of cocaine are also seized.

In each case different software is used by different people in different operating locations to contribute to common goals.

White Paper ☆ Asset Tracking Protocol

The Origins of Cursor On Target:

The cursor on Target protocol was developed in response to a known need for interoperability that became highlighted in blood by a friendly fire tragedy. The USAF employs a very highly trained subset of special forces personnel known as Combat Controllers. During an event following 9/11 while involved in operations in the Afghan theater, a Combat Control team was hit by friendly fire due to a transposition of coordinate data.

After months in the hospital, the one surviving controller was presented with a Purple Heart, and queried about what the USAF could do to prevent this. He responded that the antiquated systems needed to be replaced, and allow machine to machine targeting to help prevent human error. The genesis was a system known as Cursor On Target, which allows data interoperability and fusion data from various sources. This system now provides the Combat Controller with a digital real-time representation of the air assets at his disposal, ordnance available, along with capability for blue-force tracking of friendly forces.

The present effort is a natural progression of merging the CoT protocol created in response to a battlefield tragedy, and the OASIS protocol efforts developed in response to 911.

Summary:

1. The vision is better interoperation between federal, state and local government.
2. The focus of this paper is enabling interoperation using technology.
3. There are many operations centers. It is unlikely more operations centers will achieve the goal.
4. There are many existing information systems. It is unlikely writing more major applications will achieve the goal.
5. The many operations centers and applications do not interoperate and share data in realtime.
6. The USAF began interoperating and sharing data in realtime in the 1970's A recent protocol for this data exchange is the Cursor on Target protocol.
7. There is a standard protocol suite for interoperation between federal, state and local government. It was funded and facilitated by DHS. It is the OASIS EDXL suite (including the Common Alerting Protocol).
8. The OASIS suite lacks the functions in the USAF CoT protocol.
9. Combining the OASIS EDXL and CoT protocols creates a protocol "stack" capable of interconnecting the operations centers, warning centers, validation centers, assets and distribution centers of the USA, and the applications they use.