



**GCM ITS Priority Corridor  
Commercial Vehicle Operations (CVO) Work Group  
Transportation Security Group  
ITS/CVO Security/Funding Leadership Workshop  
Wednesday, May 12, 2004  
Argonne National Laboratory, Argonne, IL**

Meeting Notes

**Presentations from this Workshop are available on the GCM Public Information Center (PIC).**  
( [www.gcmcommunicator.com/public-library/pic-reports/pic-presentations](http://www.gcmcommunicator.com/public-library/pic-reports/pic-presentations) )

## 1. Welcome

Mr. Alan Foley, Associate Lab Director for National Security at Argonne National Laboratory, provided a general history of Argonne Laboratory. He explained Argonne's charge to help develop National, long-term homeland security initiatives, including smart sensors, infrastructure protection, and vulnerability assessments, in a comprehensive manner. He emphasized Argonne's focus on long-term sustainability for our homeland security plans and Argonne's ability to view issues that are beyond commercially available technology.

## 2. Opening Comments

Dan Shamo, GCM Executive Director, said that he hopes this workshop will help identify the security problems in current CVO systems and find solutions.

Shamo stated that in keeping with the founding principles of the GCM Corridor Coalition, the stakeholder agency level of cooperation has been our best achievement. These relationships help address institutional issues that can be as much of an impediment to effective deployment as technological issues.

## 3. Keynote Speaker

Ms. Parker, I-95 Corridor Coalition, gave a presentation entitled "Defining the Role of Regional Coalitions in Freight Security: Establishing a Framework". She noted that the I-95 Corridor originally focused on building relationships between agencies. She outlined the following objectives as a general foundation for regional freight security:

- a. Balance the need for mobility, safety, and efficiency while maintaining economic growth
- b. Fill the gap of MPO planning for multi-state corridors
- c. Demonstrate the principle that working relationships are of critical importance during severe incidents or emergencies.

- d. A key principle of National Homeland Security is that the transportation system shall be protected as a vital economic link.

She reiterated that the goal of the workshop should be defining the role and focus of the GCM Corridor in Freight Security and developing an action plan.

#### **4. Executive Roundtable**

David Zavatiero of IDOT moderated the Executive Roundtable, which featured Mike Chamness of the Illinois Terrorism Taskforce and Clifford Ong of the Indiana Counter-Terrorism and Security Council. Representatives from Wisconsin Emergency Management and Midwest Truckers Association were invited to participate but could not attend.

Mike Chamness, Chair of the Illinois Terrorism Task Force (ITTF), discussed the task force's efforts:

- ITTF originated in Fall, 1999 in response to the Oklahoma City and New York Trade Center bombing incidents, forming with 20 state agencies and 19 regions within Illinois
- The task force wants to standardize special response teams in the state. There are 7 types of Response teams: 3 state, 3 Local, and 1 Federal
- The system was recently activated when a tornado struck Utica, IL
- The Task Force has developed relationships between agencies.
- The FBI and US Attorney offices have facilitated information exchange among members to combine federal terrorism information with local information for analysis.
- Illinois has received a green rating on its preparedness plans.
- Two VACIS systems will be deployed on a pilot basis at Illinois weigh stations.
- IDOT and CDOT are jointly developing an evacuation plan for downtown Chicago. This development process will be used for evacuation plans of other large cities in Illinois.

Clifford Ong, Director of the Indiana Counter-Terrorism and Security Council, discussed Indiana's efforts to improve transportation security.

- Indiana's approach to Homeland Security is integration of these activities into other day-to-day activities. The regulatory framework currently exists to impose security initiatives.
- The motor carriers have to be in voluntary compliance with certain mandates, for example HazMat drivers licensing.
- For critical infrastructure protection, bridges are considered a high priority target, while highways could serve more as a conduit for terrorist activities. Both areas must be considered for the strategies of prevention/hardening/response.
- Another key initiative is Critical Infrastructure Monitoring using a map-based network.
- The Indiana Alert Network (IAN) is a mass-emailing system to subscribers at agencies and motor carriers.
- The technology applied must be reliable. Example: while some agencies rely on digital information technology, many first responders use analog technology. Indiana's goals for guidelines for adopting technology are:
  - The technology must be dual use and can be used day-to-day,
  - The technology must fit national standards,
  - The technology must be able to be integrated with other technology Indiana uses.

- National Standards don't exist with emergency systems.
- Information integration is a key concept, one that GCM has demonstrated well.
- Indiana has been sponsoring anti-eco-terrorism training to help respond to environmental activists targeting highway construction. Local terrorists use the same methods and procedures in preparation as foreign terrorists.
- Funding for test projects will come after vulnerability assessments are analyzed.

### Executive Roundtable Q & A Session

Dave Zavattero: Where are states heading next, and are there more institutions that need to be involved?

- Chamness: ITTF started with 20 agencies, it had 45 last year and has 60 now. However, more agencies might be needed for new issues, for example, cyber-terrorism and transport of radioactive material.
- Ong: Sustainability is the key issue for any initiative in government. Not all private sector companies understand the business case for safety and security and the expedited flow of goods as well as international companies and HazMat haulers do.

Zavattero: How good is the interaction of federal agencies (in terms of information flow) with the State on prevention initiatives?

- Chamness: Would classify as "fair, but improving". Template emergency plans exist for every Illinois county for the Threat Advisory System (the change of alert level from yellow to orange, initiating a notification structure down to local agencies). More work is needed on the communication network and command structure.
- Ong: We would recommend a 3-color threat level system. There is insufficient intelligence detail for a 5-color system.

Zavattero: Is there a coordinated approach for transportation system security with respect to standards and policy?

- Ong: Yes, within the highway agency (INDOT) framework. AASHTO is a good example of national standards that could be applied to safety and security.
- Chamness: The ITTF is sharing critical infrastructure information, but there are limited resources for what else can be done.
- Ong: Security is a manpower issue that translates into money.

Zavattero: What is the relative role of low-tech (for example Highway Watch methods) vs. high-tech in safety and security?

- Chamness: Example: Cameras are not so useful for 24-hour monitoring, but are useful for response plans.
- Ong: Solutions must be geared to the level of understanding of operations staff.

Phil DeCabooter – Wisconsin DOT: With the coming elections, agencies could realize more management turnover. How do you suggest we build a plan that survives the revolving door of management?

- Ong: It is important to have a clear mission and strategic plan. Focus on a sound safety and security business plan and industry's willingness to pay. Noted that more turnover is experienced at the local level in Indiana than at the state level.

- Chamness: Suggests looking for continuity outside of state resources, for example, private police associations and local business partners.

Zavattero: How do we get the message to the private sector to focus on the value of safety and security?

- Ong: Legislation was passed to encourage confidential business information sharing, but not many are sharing.
- Chamness: Industry wanted IL to ask them to come to the stakeholder table. More public-private partnerships are needed.

## 5. General Overview on Freight Vulnerabilities and Threats

Mark Jensen, Eric Wik, and Dan Stock of Science Application International Corporation (SAIC) discussed their experience evaluating freight vulnerabilities and threats. The SAIC presenters gave an overview of possible freight vulnerabilities and threats and rated the likelihood and potential effect of different scenarios. The threat matrix concept was outlined. The process for conducting a vulnerability assessment was reviewed as well as the Vulnerability Reduction Index. (SAIC's presentations contained proprietary information and will not be posted on the GCM Communicator.)

## 6. Discussion Circle

All attendees were given an opportunity to share their experiences and concerns relating to freight security with other attendees in a Discussion Circle forum moderated by Warren Dunham. The topic of the forum was: What is the role and focus of the GCM Corridor in freight security? Highlights of some of the significant discussion points are summarized below:

- Starnes Walker, Argonne National Laboratory: The GCM Corridor needs to determine the current gaps and a process to fill them. The Corridor Coalition should carefully map out targets and the technology that can be used to help mitigate or respond to attacks on those targets. The Corridor should link efforts to credible intelligence, reach out to technological organizations doing work in security, and jointly determine ways to mitigate threats. One activity the GCM Corridor could pursue is organizing tabletop and field exercises.
- David Zavattero, IDOT: Some activities such as vulnerability assessments are beyond the scope of the GCM Corridor, though the Corridor Coalition can still be used to share information from those activities.
- Terry Moore, Illinois DOT: We need to work on human factors as well as technology and make sure enforcement agencies evaluate security plans.
- Sgt. Paul Pershing, Illinois State Police: Key issues are education of leadership on DOT's mission in freight security, on-going training of security staff, promoting uniform methods between jurisdictions, and monitoring interstate shipments of hazardous waste.
- John Walsh, U.S. Attorney's Office: Look at what other agencies are doing to avoid duplication of effort. The corridor should be involved in the downtown evacuation plan and the First Chicago partnership.

- Jim Duncan, FEMA: FEMA is trying to bring together groups from different sectors to look at how to integrate what is being done. The Great Lakes system is a very large economic and cargo region with a variety of intersecting interests.
- Joe Ligas, Transportation Consulting Services: Areas where the GCM Corridor could address to benefit the region include integrating proprietary systems in different jurisdictions and holding multi-state tabletops.
- Bill Honan, FMCSA: ITS America is looking at including potential security initiatives in CVISN. This offers the dual use, standards, and integration requirements that Ong spoke of.
- Mike Onder, Federal Highway Administration: Approach freight advisory councils where industry and government partner, such as the CATS Intermodal Advisory Task Force (with its virtual freight team). FHWA could also help provide resources for tabletop exercises. The GCM Corridor can approach Vince Pearce of FHWA for assistance.
- Tom Hosty, Transport Service Co.: Satellite communication now being used for operations is also useful for freight security, though it needs to be developed further. The trucking industry would like to see standards developed to help determine what technologies they should invest in. Security is a major expense for small carriers. Note that keeping inventory in a manufacturing facility is more secure than keeping inventory in a container or trailer in a freight yard.
- Kevin Campbell, UPS: There is good internal communication in some shipping firms, but they need to know whom they should contact outside the organization if there is a problem. Companies need to be able to communicate information to responders.
- Dan Murray, ATRI: Don't expect much of a response when you attempt to gain industry participation, without a clear, cogent agenda on what a program offers to the industry bottom line. He feels that he currently can't articulate what GCM wants to do. Knowing what technology to buy will help truckers spend their liquid assets on something they know will last for several years.
- Marygrace Parker, I-95 Corridor Coalition: Recommended that GCM look for a simple project with an immediate payoff. One possibility is a system to exchange information that can be used every day, like the I-95 Coalition's migration to a simple web-based email notification system, giving back a simple, value-added solution.
- Dan Shamo, GCM Executive Director: The GCM Corridor doesn't know what information agencies need during an event. Push more on-demand travel information to the CVO community. Possible projects include using RWIS information to predict toxic plume spread and Virtual Weigh Stations (VWS) can serve as remote sensors.

## 7. **Funding Presentation Session** Bill Honan, Federal Motor Carrier Safety Administration (FMCSA)

Mr. Honan presented an overview and examples of potential funding sources for CVO Security projects and use of Federal Level 2 (“Expanded”) CVISN funding to support freight security projects:

- Funding options for radiological scanning devices, as tested by the Oak Ridge Laboratory:
  - Dedicated Homeland Security Funding
  - ITS Earmark Funding (50% Federal funding requires a 50% State/Local match)
- VACIS Units Obtained in Florida and Illinois:
  - Illinois used Homeland Security Funding
  - Florida used a combination of Homeland Security and State General Funding
- Alaska Hazardous Material Tracking project:
  - Used 50% ITS Earmark; 30% STIP (other Federal); 20% State funding
- Overview of CVISN program funding (according to the Administration’s SAFETEA proposal):
  - Allows for \$2.5 million per state for Core (Level 1) services
  - Allows \$1 million per State for Expanded (Level 2) services
  - The CVISN architecture should be used for all candidate projects
  - Note that CVISN funding requires a 50% match, similar to the ITS Earmark program.

Dan Murray (ATRI) voiced concern whether it was wise to pursue Expanded (Level 2) projects when we do not have national interoperability for Core (Level 1) services. Honan noted that CVISN is based on all states sharing a common base CVISN architecture to ensure that they would be interoperable. He thought pursuing Expanded projects before all Core services are implemented was justified.

## **8. Technology Solutions Overview**

Dr. Brad Micklich, Argonne National Laboratory, discussed detector technology under development. Included were radiological and nuclear countermeasures applied to commercial motor vehicle security. Passive and active detection techniques were discussed, and examples of the equipment used were provided. Passive detection, which read ambient energy from a target, is less precise than active detection, which sends a pulse into the target. Smaller detectors give less data and show less difference between materials detected.

Mike Onder, Federal Highway Administration (FHWA) discussed current security technology initiatives to enhance commercial motor vehicle operations. He noted that the Office of Freight Management’s twin focus of stimulating productivity and promoting security can often lead to conflicting actions. Best practices projects that are ongoing included the Electronic Freight Manifest, Cost/Benefit Analysis Methodology, and the Freight Business Process Map (a useful tool to identify vulnerabilities in the supply chain).

## **9. Q&A with Expert Panel**

A panel of experts moderated by Dr. Robert Gallamore of Northwestern University spoke of their experiences and answered questions from the audience. The panel participants and discussion highlights included:

Amy Houser, Federal Motor Carrier Safety Administration (FMCSA)

- Recommended conducting risk assessments, vulnerability assessments, and stakeholder forums to determine agency needs.

Tom Hosty, Transport Service Company

- Mr. Hosty noted that more carriers are concerned with cargo security than freight security. Carriers may be scared off by the perceived lack of coordination between government agencies and liability fears.

Dr. Harvey Drucker, Associate Lab Director, Argonne National Laboratory

- Economics drives the freight system
- Feels that the system is not well manifested for tracking freight containers. Any new tracking system must be able to fit the existing freight system. The freight system is an international system, not a national system, and must adapt.

Capt. Robert Powers, Michigan State Police, chair of the Transportation Security Committee of the Commercial Vehicle Safety Alliance (CVSA)

- Industry and Government need to team to achieve: Information sharing; Inclusion of industry partners; Collaboration on initiatives.

Dan Murray, American Transportation Research Institute

- The freight system is large and complex. Industry needs to work with security officials to provide them with a better understanding of the system.
- The freight system is more likely a conduit of terrorism, not a target for it.
- Government and industry need to share risk assessments
- Recommended reading is TRB Publication No. 270, describing the freight system as an essential open system for the nation's economy.
- A new cost-benefit paradigm is needed, where the beneficiary pays. If there are public benefits for an initiative, the public should pay.
- The nation needs a common CVISN system or interoperability between states.
- Digital tracking of cargo information data is a promising trend.
- Some recommendations for the GCM Corridor:
  - 1) Focus on an integrated, 3-state CVISN System;
  - 2) More outreach is needed to have better representation for the Midwest in the security area;
  - 3) Complete some cutting edge operational tests;
  - 4) A layered redundancy is needed for the planned system.

Ron Char, Johns Hopkins University, Applied Physics Laboratory

- Security will need to be enhanced through security because there is not enough manpower to cover the entire system. Building several smaller interrelated components of a system is more effective than making a single complex system.
- GCM needs to decide what needs to be done, who does it, and what the desired outcome is.

Dr. Gallamore asked the panel what they thought the biggest priorities were.

Dan Murray: The surface transportation system has found itself in the middle of the security dilemma.

Dr. Drucker: The number of possible threats far exceeds the available resources. There is only a still-evolving sense from DHS on priorities for a very difficult problem. Apply basic science first to develop proven technology second.

Tom Hosty: Some mandates are so massive that they can hurt the industry. The cost of complying with Commercial Driver's License HazMat rules are having a severe adverse affect on the industry.

## 10. Action Plan for GCM Led by Dan Shamo

Workshop participants provided input to develop the framework for short (1-2 year) and long (5 year) term Action Plans with milestones. The resulting end product was a MindMap application outline that served as the initial framework for a GCM action plan. The document will be posted on the GCM Communicator.

### Participants

First Name	Last Name	Agency/Company
Kevin	Campbell	UPS
Mike	Chamness	Illinois Terrorism Task Force
Joe	Chaney	FBI
Ronald	Char	Johns Hopkins University
Brian	Daugherty	Bulkmatic Transport Company
Phil	DeCabooter	Wisconsin DOT
Harvey	Drucker	Argonne National Laboratory
Jim	Duncan	FEMA
Warren	Dunham	Warren B. Dunham Associates
John	Ellis	TranSmart Technologies, Inc.
Tom	Ewing	Argonne National Laboratory
Izabela	Flis	Illinois DOT
Alan	Foley	Argonne National Laboratory
Robert	Gallamore	Northwestern University
Ken	Glassman	ITS Midwest
Jeff	Hochmuth	ITS Midwest
William	Honan	Federal Motor Carrier Safety Administration
Tom	Hosty	Transport Service Company
Amy	Houser	FMCSA
Mark	Jensen	SAIC
Laura	Krooss-Wiley	Schneider National Carriers, Inc.
Paul	Lamb	URS
Dave	Lazarides	Illinois Commerce Commission
Joseph	Ligas	Transportation Consulting Services
Warren	Lutz	Federal Highway Administration
John	Maes	Highway Watch Illinois
Jeff	McSpaden	Federal Highway Administration
Brad	Micklich	Argonne National Laboratory
Terry	Moore	Illinois DOT
Daniel	Murray	American Transportation Research Institute/ATA

Mark	Newland	Indiana DOT
Mike	Onder	Federal Highway Administration
Clifford	Ong	Indiana Counter-Terrorism and Security Council
Promise	Otaluka	Federal Highway Administration
Dave	Pabst	Wisconsin State Patrol
Marygrace	Parker	I-95 Corridor Coalition
Bill	Parks	Professional Towing & Recovery Operations of Illinois
Jim	Peerenboom	Argonne National Laboratory
Paul	Pershing	Illinois State Police
Robert	Powers	Michigan State Police
Brian	Quirke	US Department of Energy
Gary	Rylander	ITS Midwest
Gary	Schenkel	TSA
John	Schneider	Argonne National Laboratory
Dan	Shamo	URS
Chuck	Sikaras	Illinois DOT
Bob	Sproule	U. S. Customs Border Protection Service
Dan	Stock	SAIC
Adrian	Tentner	ITS Midwest
Christine	Van Horn	Department of Energy
Wes	VanBurggen	A and R Transport
Starnes	Walker	Argonne National Laboratory
John	Walsh	U. S. Attorney's Office
Erik	Wik	SAIC
Pat	Wilkey	Argonne National Laboratory
Sam	Wolfe	Indiana DOT
David	Zavattero	Illinois DOT