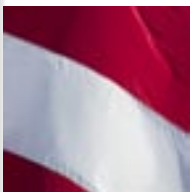
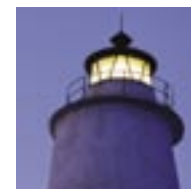


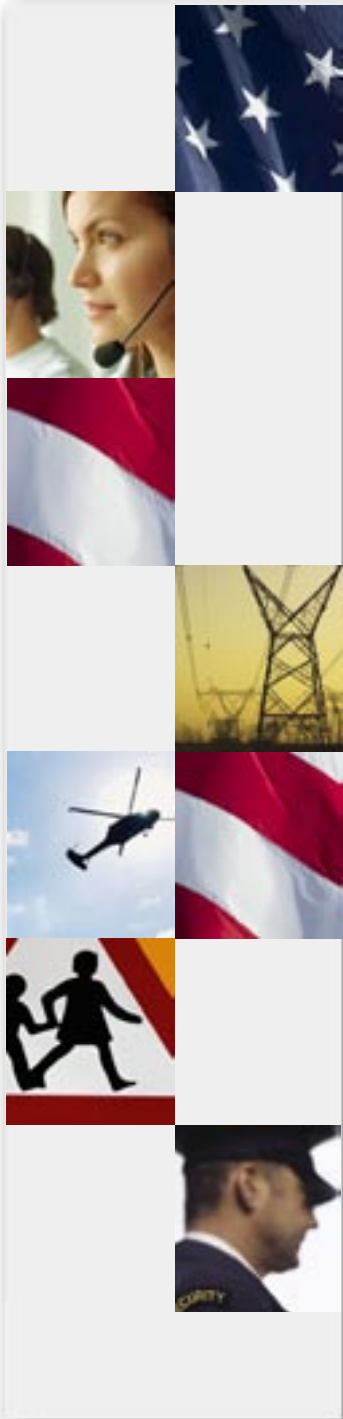
Mid-Atlantic All Hazards Forum 2007

Post-Conference Report



Report sponsored by IBM





Contents

Preface

- ▶ All Hazards Forum and Consortium 3
- ▶ Special thanks 7
- ▶ 2007 Forum overview 8
- ▶ About the sponsor 10

Session categories

- ▶ Opening plenary session: Homeland security directors' roundtable 12
- ▶ Border, transportation, urban and campus security 16
- ▶ Critical infrastructure protection 29
- ▶ Emergency management 43
- ▶ Grants and procurement 64
- ▶ Health and medical readiness 69
- ▶ Information sharing and intelligence 79
- ▶ Law enforcement 88
- ▶ Public safety communication and interoperability 93

Resources

- ▶ Contacts 103
- ▶ Presentations 103
- ▶ Web links 103

The All Hazards Forum and All Hazards Consortium – evolving to better meet the needs of the community

What's new for 2007

The past year has seen both stabilization and evolution for the All Hazards Forum and All Hazards Consortium. The 2006 All Hazards Forum's format worked so well that it was kept largely unchanged from the 2007 forum, with parallel tracks of closed "meeting of meetings" sessions and open discussion panel sessions. The number of attendees was kept approximately constant as well.

Regional workshops and white papers

While the Forum has kept its winning formula, the other activities of the Consortium have evolved. The most notable change has been a new series of focused regional workshops. This idea came out of the 2006 Forum, and has proven highly successful. The Consortium is applying its core expertise of bringing constituent groups together to facilitate the meetings. These workshops focus on a single issue and are thoroughly documented. The result of each workshop is a white paper that, in addition to spreading knowledge and best practices about the topic, contains the seeds for new research initiatives.

The university sector has both enabled and benefited from the regional workshop concept. Universities have become the facilitators of the regional workshops, providing facilities for meetings, alerting and engaging their private sector partners to get involved with the Consortium and, perhaps most importantly, documenting the workshops and creating the

white papers. These white papers are a valuable resource, because they contain the seeds for new research projects that the universities can use to apply for increasingly scarce grant funding. The Consortium, then, is helping to drive research by creating the justification for research.

The regional workshop concept is also proving of interest to federally funded research and development centers – groups like the RAND Corporation and the MITRE Corporation. These groups have been increasingly involved with the Consortium's activities over the past year.

Expanding the Consortium concept

In past years there has been an effort to expand the All Hazards Consortium concept to other regions around the country. However, it has become evident that because of different cultures and dynamics across the nation, the idea of copying the model that has proven so successful in the mid-Atlantic region and applying it elsewhere is not viable. As a result, the Consortium has shifted focus and is now working to export the principles that underlie the Consortium and Forum, so that other regions can possibly adopt them and create their own collaborative organizations and initiatives. The regional workshop with its freely available white paper findings, is one of the first such efforts. Other paths, such as podcasting and television production, are also being considered.

[All Hazards Forum and Consortium overview](#)[Special thanks](#)[2007 Forum](#)[About the sponsor](#)

Sustainability

As noted in the Forum overview, sustainability has become a top-of-mind issue. Sustainability involves ongoing funding of all-hazards initiatives, but it goes beyond money. There are three basic areas of focus to keep preparedness on track:

- *Focus* – Any endeavor as large and complex as all-hazards planning and preparedness is subject to scope creep and complacency. It is necessary to continuously engage, and keep on covering the same topics. Past successes, lessons learned and best practices must be rolled into future efforts. Momentum is critical.
- *Engagement of the private sector* – This area of focus is critical. After 9/11, grant money drove all-hazards initiatives, and there was a high degree of interest. While grant funding is still a major consideration, it is becoming more scarce. For this reason, the private sector must become involved. They have funding, but in order for it to be spent, projects and initiatives have to become a business development tool. This should become a key consideration going forward.
- *Continuity of leadership* – As time passes, those who had been driving preparedness are moving on to other careers, getting voted out of office or retiring. In order to prevent the loss of their expertise, the Consortium has been working to keep them involved with the Consortium itself. The Consortium is also changing its target audience to maintain continuity. In government, there are three tiers of professionals: executives in the top tier, appointees in the mid tier and “lifers” – civil servants – forming a base of support.

The Consortium started by targeting the mid tier, but has concluded that it should broaden its focus to address those who will be on the job long after those appointees have been replaced – the “lifers.”

[About the All Hazards Forum and other All Hazards Consortium activities](#)

In 2004, Homeland Security officials from the National Capital Region saw a need to create an event that would cross organizational and institutional boundaries, bringing a broad-based group of stakeholders in hazards preparedness, response and recovery, and homeland security together to exchange ideas and best practices, develop lasting relationships and foster an ongoing dialogue that would benefit all.

The officials noticed that the stakeholders were already attending conferences and meetings to discuss these problems, but for the most part they were meeting only with their peers: police chiefs were going to law enforcement conferences, transportation officials were going to transportation conferences, and so on. There was no single place where communication was taking place between these silos.

The idea of a conference for the mid-Atlantic region (NC, VA, WV, DC, MD, PA, DE, NJ, and NY) was born. The first All Hazards Forum in 2004 was a great success, providing an opportunity for government, industry and universities to meet face-to-face.

[All Hazards Forum and Consortium overview](#)[Special thanks](#)[2007 Forum](#)[About the sponsor](#)

The Forum, in conjunction with the Consortium's other activities during the year, brings together several distinct constituencies, each one of which has different capabilities and needs:

- *Government* – Government “owns” the problems surrounding preparedness and homeland security, as well as some of the funding to solve those problems...but government does not have solutions *per se*.
- *Private sector* – The private sector creates solutions, products and services that government needs to solve its problems. Also, critical assets are often owned by private companies, such as railroads, shipping companies and utilities. Other companies with an interest in homeland security and preparedness, such as financial institutions and insurance providers, are also part of this group.
- *Universities* – The universities bring independent knowledge and expertise to the equation, helping determine what solutions are appropriate. Government may need solutions, but doesn't necessarily have the ability to clearly define what those solutions may look like. Universities provide key resources in the form of centers of excellence.
- *Not-for-profits* – These stakeholders provide access to information and people who are focused on a particular segment of the all hazards problem.

In addition to validating the basic idea of a cross-disciplinary regional meeting, the first All Hazards Forum spawned an ongoing outreach effort in the form of a series of conference calls that serve to help maintain contact throughout the year, giving interested parties a chance to hear about the latest best practices, new challenges and ongoing needs. The conference calls proved very useful as a way to cross organizational boundaries and foster communication and collaboration within the mid-Atlantic region. The public calls were scaled back in 2007 to better focus on other activities, but are expected to ramp up again in 2008. Private conference calls with targeted audiences have kept up their pace, however.

As noted above, in addition to the conference calls, the Consortium has implemented a series of regional workshops on specific topics. These working sessions have been very successful and the white papers that result from them have proven very useful in driving new research initiatives.

One of the annual goals of the AHF is to help collect information shared and distribute it across the U.S. to all states in order to help improve overall knowledge and coordination at the regional level. To accomplish this, the All Hazards Forum Annual Report is published, which summarizes the activities and lessons learned during the conference. It is a practical document that clearly communicates the issues and strategies in homeland security and emergency management as well as best practices and lessons learned from real disasters. The AHF Annual Report also serves as a working document for all stakeholders to learn about the region's issues, challenges, opportunities and solutions.

All Hazards Forum and
Consortium overview

Special thanks

2007 Forum

About the sponsor

About the All Hazards Consortium

The All Hazards Consortium (AHC) was originally conceived as an extension of the All Hazards Forum, formed to support the ongoing interactions between stakeholders, further the goals of the Forum and provide support to homeland security and emergency management efforts. Since its inception, the All Hazards Forum has been a grass-roots effort, formed on an ad-hoc basis and adapting as needed to best serve the needs of its constituents.

Led by a board of directors from both government and private sectors, the AHC has the following goals:

- To create a multi-state network of people from government, the private sector, universities and non-profits.
- To act as a facilitator, creating an appropriate environment for government, industry, universities and non-profits to come together to discuss issues, share best practices/ideas/strategies and discuss plans to improve regional coordination between all stakeholders.
- To develop and implement a process for collaboration, using proven, effective tools such as meetings, conference calls, symposiums and workshops, combined with professional planning and facilitation skills, to help generate results that lead to improved regional readiness.
- To help identify, clarify and prioritize state/local government requirements for homeland security and emergency management initiatives.

- To provide education, training and certification services through year-round activities.
- To provide a vehicle that could create multiple conferences across the U.S. to meet the needs of other regions.
- To help stimulate regionally coordinated planning, programs and procurements.

The All Hazards Consortium was built on the belief that state/local government is ultimately responsible for the protection of the public, but that it is critically important to involve all stakeholders – government, the private sector and universities/not-for-profits. By bringing together all stakeholder groups into regional advisory committees, working groups and ad hoc committees, and focusing on specific issues (with state government driving the needs), a powerful environment for collaboration is created to solve tough problems that require resources from every sector.

This “culture of collaboration” is what creates the energy that drives the All Hazards Consortium and its supporters to work together to protect the region’s citizens from all types of hazards.

For more information

Contact the All Hazards Consortium at: www.ahcusa.org for more information. Or, to reach out to the Consortium leadership, visit www.ahcusa.org/leadership.htm

Special thanks to:

Governor Martin O'Malley and the host state of Maryland

Bob Crouch

President of the All Hazards Consortium Assistant to the Governor for Commonwealth Preparedness, Virginia

John Contestabile

Chairperson of the All Hazards Consortium Advisory Committees, Director, Office of Engineering, Procurement and Emergency Services, Maryland Department of Transportation and Chair, Regional Advisory Committee

Tom Moran

Executive Director of the All Hazards Consortium Commercial Services Network and AHF Government/Industry/Public and Private Sector Liaison

IBM is again proud to be the sponsor of the 2007 Mid-Atlantic All Hazards Forum (AHF) report. As the All Hazards Consortium strives to make each year's Forum better and better, we think you will find a wealth of new and updated information inside this year's report as well.

We would also like to thank the organizers, participants and attendees of this important event – all those who represented our federal, state and local government, private industry, and the not-for-profit and university sectors. Your far-sightedness and dedication to this cause, and your willingness to sit down and try to find a practical approach to the issues facing our nation today and address them, serve as an inspiration to us all.

We hope you will find the report interesting and informative.

How to navigate an interactive PDF: Due to the large amount of information in this report, it is presented in the form of an interactive PDF, which contains the usual navigation tools, such as the right-hand scroll bar or navigation arrows at the bottom of the page. Additionally, you can:

- Click on any of the tabs at the top of the page to move from section to section.
- Click on any of the live links on the page, or use the left-hand navigation bar to move between sessions and between focus areas.

[All Hazards Forum and Consortium overview](#)[Special thanks](#)[2007 Forum](#)[About the sponsor](#)

The 2007 All Hazards Forum was held in Baltimore, Maryland, on November 7-8, 2007, and drew an audience of approximately 1,000. Attendees were offered more than 40 conference sessions and private meetings, and more than 90 panelists.

All Hazards Forum 2007 overview

The Forum continues to evolve based on feedback and lessons learned from earlier events. For 2007, the panel discussion focused on eight areas:

- Border, transportation, urban and campus security
- Critical infrastructure protection
- Emergency management
- Grants and procurement
- Health and medical readiness
- Information sharing and intelligence
- Law enforcement
- Public safety communication and interoperability

Focusing on all three phases of a hazard: readiness, response and recovery, the All Hazards Forum's mission is to help build communication and relationship between the states in the mid-Atlantic region (NC, VA, WV, DC, MD, PA, DE, NJ, and NY) through a year-round program of sustained interactions between its stakeholders.

All Hazards Forum and Consortium overview

Special thanks

2007 Forum

About the sponsor

In 2007, the trend towards special private sidebar meetings continued. This “meeting of meetings” concept enables the AHF to become a venue to hold meetings that would otherwise have to be conducted separately, thus encouraging valuable information exchanges and facilitating introductions to key players in the government, industry, education and non-profit sectors. By concentrating these meetings in time and space, far more can be accomplished in far less time, and at less expense.

[Common themes](#)

In 2007, cooperation/coordination, interoperability and planning/practice were still high priorities for participants. Issues that came out much more strongly in 2007 were sustainability, how to deal with shrinking budgets and how to insure continued funding. A number of panelists alluded to increasing apathy affecting momentum of existing programs and initiatives, but the overall tone was positive and constructive. An overarching theme once again in 2007 is that of relationship building and communication. Time and again, panelists spoke of the need for better relationships among stakeholders, better follow-through and better management of programs. This highlights the importance of the All Hazards Consortium’s mission of facilitating relationship building and collaboration, and engendering trust.

[About this report](#)

The purpose of this post-conference report is to provide a concise, useful summary of the conference, rather than an exhaustive compendium. All of the public panel discussions and plenary sessions are covered, with insights that were presented during the course of the conference. For those who wish additional information, there are links throughout the document and a reference section designed to guide the reader to the relevant resources.

All Hazards Forum and Consortium overview

Special thanks

2007 Forum

About the sponsor

IBM

IBM Corporation
100 E. Pratt Street
Baltimore, Maryland 21202
U.S.A.

Peter Porter
Certified Client Executive
IBM Public Sector
410 332-2262
pporter@us.ibm.com
www-03.ibm.com/industries/government
www-03.ibm.com/industries/education
www-03.ibm.com/industries/healthcare

The challenge

Today, state and local governments, public safety agencies and education officials are faced with many challenges when dealing with the issues of safety and security. Whether dealing with natural or man-made threats, those responsible for the safety and security of citizens are challenged with the difficult task of keeping their physical and IT environments safe.

With lives and economic viability at stake, governments, public safety agencies and schools must be willing to make changes within their infrastructure, safety and security systems, and emergency response strategies to proactively address threats so that they can respond effectively when situations arise.



IBM provides solutions that address these critical needs.

- Physical Security and Surveillance
- Digital Video Surveillance
 - Remote Asset Tracking, Biometrics, RFID and Barcode Security

- Crime Analysis, Threat and Fraud Intelligence Solutions
- Crime Data Warehouse
 - Threat and Fraud Intelligence

- Emergency Response Planning and Collaboration
- Wireless Infrastructure
 - Emergency Response Networks
 - Rapid Response Infrastructure

- IT Security
- Single Sign-on
 - Internet Security Solutions

IBM differentiates itself from competitors by offering clients a unique portfolio of public safety and security offerings designed to take existing assets and integrate them into a comprehensive solution that addresses the most pressing safety and security issues.

By utilizing a comprehensive portfolio of hardware, software and services and incorporating cutting-edge research and development assets, IBM is able to take its clients from design and development through implementation and ongoing management of the most demanding solutions. No other vendor has the same fully integrated end-to-end capability.



Session categories

- ▶ Opening plenary session: Homeland security directors' roundtable
- ▶ Border, transportation, urban and campus security
- ▶ Critical infrastructure protection
- ▶ Emergency management
- ▶ Grants and procurement
- ▶ Health and medical readiness
- ▶ Information sharing and intelligence
- ▶ Law enforcement
- ▶ Public safety communication and interoperability

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Opening plenary session: Homeland security directors' roundtable

Panelists

John Droneburg
Director, Emergency
Management, Maryland

Robert P. Crouch, Jr.
Assistant to the Governor
for Commonwealth
Preparedness, Virginia

David Mitchell
Secretary of Public Safety
and Homeland Security,
Delaware

James W. Spears
Homeland Security Advisor,
West Virginia

James F. Powers, Jr.
Director of Homeland
Security, Pennsylvania

Darrell L. Darnell
Director of the District of
Columbia Homeland
Security and Emergency
Management Agency

William Bowen
Health Policy Advisor,
New York State Office
of Homeland Security

The opening session of the Forum brought homeland security and emergency management officials from all the states in the region together to present an overview of their current situation and activities, what they've done in the past year, and what challenges they face going forward.

Highlights

Maryland

- 2007 brought a change of administration in Maryland. The new governor launched some broad initiatives to gain a clear understanding and definition of various issues.
- The first area of focus was assessment. State emergency management and homeland security officials were directed to work closely with local jurisdictions to define what the major issues (12 specific areas of interest based on national priorities) mean in real terms. Once defined, the current status was measured against standards of readiness to find gaps and opportunities for improvement. This process was still ongoing at the time of the conference.
 - The example used was interoperability. The agreed-upon definition was that every local jurisdiction have a digital radio system capable of talking to all first responders, capable of allowing first responders talk to one another and capable of communicating with neighboring jurisdictions. Even at this basic-definition level, Maryland has not achieved interoperability.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

•The second area of focus was information sharing. Exactly what is meant by a “fusion center,” what functions does it serve and how does it connect to federal, state and local agencies? There are multiple programs and the state has been working to put all the pieces together. Ensuring that information is accessible is key.

•The third area of focus was sustainability, in terms of both funding and momentum. Shrinking federal grant dollars and budget deficits are a serious issue. Also, maintaining public awareness is critical to preparedness.

Virginia

•In 2007, Virginia implemented a regional approach to gain local stakeholder (practitioner) input, adopting a bottom-up philosophy when defining initiatives and allocating resources.

•Campus security was a focus in 2007, in large part because of the April shooting at Virginia Tech. A Higher Education Preparedness Consortium similar to the All Hazards Forum was already being built up at the time of the shooting. Its goals are similar to those of the AHC, but targeted at educational institutions. After the shooting a campus security conference similar to the All Hazards Forum was held.

•Virginia is working with educational institutions to help develop degree programs in homeland security, hoping to create professionals interested in entering the field.

•In 2007, a baseline survey of interoperability at the local level was established, in part to provide input for the one-time Public Safety Interoperable Communications (PSIC) grants that are designed to help leverage the newly reallocated 700 MHz spectrum.

•Virginia has launched a public awareness program called the Ready Virginia Campaign to help develop a culture of preparedness.

•Continuation of post-Katrina work, particularly in the sheltering area, was conducted.

•Collaborative outreach with neighboring states was expanded and is ongoing.

•Sustainability from a budgetary standpoint is also a challenge for Virginia.

Delaware

•Delaware has accomplished near-total radio coverage in the 800 MHz band outdoors, and approximately 75 percent coverage indoors. The state is in the process of testing major infrastructure for indoor coverage, and has passed a law that requires 800 MHz testing in new commercial buildings, and if it is not achieved, the installation of equipment to provide coverage.

•Delaware is focused on disaster recovery, specifically how to restore communications resources such as radio towers.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- The Delaware Information and Analysis Center (DIAC, the state's fusion center) is approaching full 24x7 coverage with the addition of more personnel. In addition, new relationships are being forged with the healthcare and fire fighting communities to enhance its capability.

- Medical surge capacity is a concern. New equipment has been purchased (a medevac helicopter), and planning is ongoing to handle a major medical event such as an H5N1 outbreak.

- Work is being done to improve data communications interoperability to complement voice interoperability.

- A critical asset inventory database project is underway.

- A public outreach program targeting the VFW has been launched to try to capture some existing expertise on a volunteer basis.

- Maritime security is a looming challenge. Equipment is old and in marginal condition, and a liquefied natural gas terminal will be built sometime in the next few years, either in Delaware or in upstream states.

West Virginia

Note: Due to technical difficulties, a significant portion of Mr. Spears' comments were not captured.

- West Virginia is concerned with the ripple effect of a disaster (consequence management) and the interdependencies among neighboring states. Evacuation planning has been a focus.

- The impact of events is not necessarily proportional to population. West Virginia has a relatively small population, but will be powerfully impacted by an evacuation of the NCR.

- An evacuation simulation project is being developed, using computer simulation that can work with real-time actions. It will have a regional focus, in keeping with the state's consequence management priority.

- The development of an all hazards mindset is an ongoing challenge. FEMA, for example, is focused on hurricanes, but West Virginia has had major flooding events that have not received the same level of attention.

Pennsylvania

- Pennsylvania has significant challenges surrounding information sharing, and has no fully operational fusion center, but progress is being made. An important part of the challenge is Pennsylvania statutes that block the sharing of criminal investigative data with non-law enforcement personnel. This is also a cultural issue.

- Pennsylvania has completed the identification of critical infrastructure in accordance with the National Infrastructure Protection Plan (126 sites) and is moving on to assets that meet the criteria of its own state infrastructure protection plan (an additional 325 sites).
 - All schools are deemed critical infrastructure and are not included in these numbers.
 - Currently underway is an effort to assess vulnerability at these sites.

Opening plenary session: Homeland security directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Maritime security is an ongoing priority, and new equipment has been purchased.
- A new protocol has been put in place to classify data so it does not get out into the public domain.
- A key ruling was made concerning funding for first responders. Federal funding is split between local and state agencies on an 80/20 basis, but in many Pennsylvania municipalities there is no local police force; the state police are the only agency. The ruling makes the state police eligible for those local funds.
- An initiative to develop a food safety and security strategy is underway.
- Pennsylvania is also reaching out to colleges and students, and launched an internship program.

District of Columbia

- DC noted information sharing and funding as key issues. DC has unique funding challenges.
- The DC fusion center (Washington Regional Threat Analysis Center) is working closely with other fusion centers on an ongoing basis.

New York

- New York has opened a training center to provide multidisciplinary, cross-functional, cross-jurisdictional training.
- Public education and developing a self-reliant mindset was identified as a challenge.

- A prototype system to bring critical infrastructure experts together with intelligence analysts is being evaluated (Critical Infrastructure Suspicious Activity Reporting), to "connect the dots" and avert attack.

Resources

Delaware

dshs.delaware.gov/

District of Columbia

hsema.dc.gov/dcema/site/default.asp

Maryland

www.gov.state.md.us/gohs/index.asp

New Jersey

www.state.nj.us/njhomelandsecurity/

North Carolina

www.nccrimecontrol.org

Pennsylvania

www.homelandsecurity.state.pa.us/

Virginia

www.commonwealthpreparedness.virginia.gov/

West Virginia

www.wvdhsem.gov/

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Border, transportation, urban and campus security

- ▶ Campus safety and security
- ▶ Access control and Transportation Worker Identification Credentials
- ▶ Urban Area Security Initiative
- ▶ Transportation operation centers and their role in homeland security

Opening plenary session:
Homeland security
directors' roundtable

**Border, transportation,
urban and
campus security**

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Campus safety and security

Moderator

Cheryl Elliott
Institute for Infrastructure
and Information Assurance,
James Madison University

Panelists

Robert Lang
Assistant Vice President for
Strategic Security & Safety,
Kennesaw State University,
Kennesaw, Georgia

In light of the recent mass murder at Virginia Tech, public safety directors are reviewing their campus security plans and discussing best practices to prevent such tragedies going forward.

Highlights

- James Madison University (JMU) has been focused on campus safety and security since Y2K; the shootings at Virginia Tech have heightened awareness and intensified discussion, as they occurred “just down the road” from JMU.
- At JMU, in an emergency situation, all of the decision-making authority rests with the campus police, specifically the chief. The decision to call in HAZMAT teams, or to request help from other jurisdictions lies with the campus police, as does the decision to cede authority to any reinforcement that may have been requested.
- Dealing with the press or disseminating information to the community at large – beyond the university – is the responsibility of the public information officer.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- JMU would be considered the third-largest city in its region, and hence is virtually impossible to shut down. Instead, it has divided its campus into five zones, each of which could be individually closed off and still allow the university to function as a whole.
- The five zones are: the village, lakeside, blue stone, hillside and seaside. Knowing that part of the campus can close and the rest can still operate is important, and it raises some very interesting questions such as:
 - How do you determine if that campus can operate with one or more zones closed?
 - Just what are the critical infrastructure assets on campus?
 - Is there a priority to defining them and protecting them?
 - How does an institution prepare for protecting those assets?
- Once JMU decides a safety and security issue needs to be addressed, it has a number of ways to inform its community. Noted Elliott, "One thing JMU feels strongly about is that using text or voicemail messaging for emergency notification *alone* is not a silver bullet." At JMU, for example, there are about 20,000 people in the community, with about 16,000 students, and those people need to opt in either to receive voicemail or text messaging. Currently, they only have about 8,000 users registered, so it is not a campus-wide communications solution. And standard rates apply – to send a message to 8,000 people would cost approximately US\$800, so is not an economically feasible solution.
- In the case of an emergency, JMU uses a variety of ways to communicate with the JMU community: an AM radio station, Web pages, blast e-mails, text messages, building coordinators, the residence hall staff, phone trees, emergency fax notification, police loud speakers and PA systems, the Thorguard Lightning Prediction System – a long 15-second air blast – and local media such as campus TV radio broadcast.
- One lesson learned from the Virginia Tech tragedy was to put a blocking page on the JMU Web site. The Virginia Tech server could not handle all the external traffic and crashed; in the event of an emergency, the JMU Web site would continue to function internally, and be impervious to external queries.
- Robert Lang pointed out that all evacuation plans must be tested, and all plans of any major towns or businesses on the perimeter of a university must be tested as well, to ensure there are no conflicts in evacuation techniques.
- Lang also noted that many campus "shooters," beginning with Charles Whitman at the University of Texas in the early 1960s, were actually known to campus authorities. Lang stated that Whitman actually saw a psychiatrist at the University of Texas the day before the mass murder and in essence was "blown off," and so he decided to commit the mass murders the next day. Lang noted that there were similarities in the Virginia Tech case.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Lang noted most people involved in campus security have some knowledge of Family Education Rights and Privacy Act (FERPA) which restricts administrators from sharing student information with the police department or anyone else unless an emergency clause is enacted. The emergency clause normally means you have to have a person almost in the act before you can do anything about it. Essentially, this is what allows many campus shooters to slip through the cracks and commit atrocities.
- At Kennesaw State University, they have deeply researched FERPA, and believe that the act allows more opportunity to do some things proactively than most people think. Lang urged all participants to research the act more closely.

Resources

James Madison University public safety
www.jmu.edu/pubsafety

Opening plenary session:
Homeland security
directors' roundtable

**Border, transportation,
urban and
campus security**

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Urban Area Security Initiative

Moderator

David MacMillan
COG UASI Project Manager

Panelists

Charles Madden
Acting Grants Division
Chief, DC Homeland
Security and Emergency
Management Agency

William J. Goodwin, Jr.
Chief, Baltimore City
Fire Department

Ken Wall
Deputy Director, Office
of National Capital
Region Coordination

Douglas Fassbender
Contracting Specialist,
New York State Office of
Homeland Security

The Urban Area Security Initiative (UASI) is a federal program designed to provide funding to homeland security-related programs in designated urban areas. UASI is divided regionally and also by tiers, with major metropolitan areas (e.g., New York) falling into the top tier and smaller urban areas (e.g., Buffalo) falling under Tier 2. Partners in a UASI group may be made up of several cooperating stakeholder entities, ranging from city and county governments to administrative entities such as the Port Authority of New York.

While the program as a whole provides funding, it is up to each region to develop proposals, administer the grant process and determine how UASI fits into existing administrative structures. With many millions of dollars involved, governance is an important issue. There is no single administrative model, and different groups operate in different manners. This panel explored how several mid-Atlantic UASI groups are governed.

Opening plenary session:
Homeland security
directors' roundtable

**Border, transportation,
urban and
campus security**

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Highlights

- UASI is usually administered by pre-existing organizations, or by offshoots of those organizations. While the details of governance are left up to each UASI group, governance structures are typically layered, with local practitioners/subject matter experts at the bottom, one or more coordinating committees comprising middle layer(s), and a senior policy group at the highest level.
 - There may be advisory groups with the ability to provide input that are not part of the governance structure itself.
 - Governance structures are rarely if ever pre-defined; rather, they evolve. Governance can be a laborious, complicated process. Finding ways to streamline it is a priority.
 - The purpose of the coordinating committees/organizations is to manage and navigate a complex patchwork of funding programs, federal and state mandates, jurisdictions and stakeholders.
 - Keeping projects on schedule and on budget is an additional function of UASI governance.
 - Some projects initially created under UASI take on a life of their own and require their own governance structures.
- Given the large number of stakeholders in each UASI group, aligning priorities, resources and policies can be a major challenge.
- UASI grants and the initiatives they fund do not exist in a vacuum. UASI grants must be coordinated with other funding sources, and all mandates must be complied with.
- UASI groups must justify funding on an ongoing basis. The example cited was Buffalo, N.Y. Initially a full UASI partner in its regional group, the city did not articulate its position very well and was put on “sustainment” status until it was able to demonstrate the importance of spending in the area.
 - Sustainability is an issue with investment justification. Other sources of funding, such as subscriber fees, are one way to ensure continuance of some initiatives.
- Investment justifications developed by UASI groups are often very similar from region to region (e.g., citizen/community preparedness, interoperable communications), but because of the unique needs of each region some are very location-specific (e.g., the Lower Manhattan Security Initiative, the Canadian Border Security Program).
- Neighboring UASI groups should consider cooperating when developing investment justifications that can benefit both groups (e.g., Buffalo and Detroit jointly proposing enhancement of the Canadian Border Security Program).

Opening plenary session:
Homeland security
directors' roundtable

**Border, transportation,
urban and
campus security**

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- UASI can help make better use of resources.
 - Initiatives can be leveraged by bringing diverse stakeholders together. The example cited was the use of cross-disciplinary training.
 - UASI can provide the impetus to determine how well existing capabilities meet urban security initiatives, so that rather than “reinventing the wheel,” UASI funds can be used to enhance what is already in place.
- Administering grant funding is done in some areas through Web-based “e-grant” systems. There is no single, common system. Typically, these systems cover all available grant programs, and provide a way to submit funding requests and track status.

Resources

UASI Portal
secure.cityofno.com/Portals/UASI/portal.aspx

Contact information

To view e-grants demo site:
Fernando Lagunes, 410-320-3237

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Access control and Transportation Worker Identification Credentials

Moderator/Panelist

Sylvia Floyd-Kennard
Director of Human
Resources and Security,
Port of Wilmington,
Delaware

Panelists

Andy Engemann
Chief of Police, Virginia
Port Authority

Patrick Hemphill
Security Manager, Port of
Wilmington, Delaware

Iana Bohmer
Northrop Grumman

Secretary of Homeland Security Michael Chertoff stated on February 5, 2007 that the FY 2008 budget includes US\$26.5 million for the Transportation Worker Identification Credential (TWIC), to enhance worker identification and security at our nation's ports and critical transportation facilities. The Port of Wilmington, Delaware is set to pilot the launch of the TWIC program.

Highlights

- In 2003, The Port of Wilmington was contacted by Transportation Security Administration (TSA) and was asked if it would be a pilot site for the TWIC card. It agreed to do so.
- In common usage, TWIC is pronounced "twick" and going through the process to obtain a TWIC card is known as being "TWICed." (pronounced as "twicked.")
- Initially, the port issued about 3,500 test cards to employees and truck drivers. It was voluntary. The cards worked with readers installed at gates and turnstiles for the workers. It did speed things up and people who wanted to move along quicker jumped to get the card. With no background check involved the only thing they had to do was supply their name.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- In 2005, TSA began issuing the prototype card, and that required workers getting fingerprinted and having their name checked against the "No-Fly" List. The fingerprint was the first (and to date, only) biometric used.
- When the "final" cards were announced, and it was clear they would begin to be issued March 26, 2007, many issues were raised.
- Employees were concerned about the depth and breadth of background checks, and tenants of the Port wanted to know who was footing the bill for the cards and the background checks.
- The port has warehouse workers and deep-sea workers. Basically, deep-sea workers take products or the commodities from the ship to the first point-of-rest, and warehouse workers take products from the first point-of-rest to warehouses. One problem for the port was that the majority of its workers had "checkered pasts."
- There are disqualifying acts that prevent a person from working. Some of the acts can be waived and that worker would be permitted to work. Once workers finally realized that TWIC was going to be a reality, they knew they were going to have to do something to ensure that they could keep working.
- Union leaders – both deep-sea and warehouse workers – forged a partnership to try to facilitate getting pardons/ waivers for some people. Unfortunately, this takes time.
- The advice given was to be proactive.
- Prior to it becoming mandatory to have the workers TWICed, any employees who may have had a checkered background were told to register for TWIC early. Then they could go through the appeal process; until the compliance date kicked in, they could continue to work and appeal. After the mandatory compliance date, workers had to have a TWIC card to work.
- The background check covers a period of only seven years, except for extreme offenses such as acts of terror. Everything is appealable.
- The TWIC check and appeal process is similar to the one already in place for HAZMAT drivers. Only one percent of HAZMAT drivers who applied did not qualify to get their licenses after their waiver and appeal process.
- The TWIC card itself is similar to the Federal Employee HSPD-12 card and is based on the FIPS 201, which is the standard relating to Homeland Security Presidential Directive 12.

Opening plenary session:
Homeland security
directors' roundtable

**Border, transportation,
urban and
campus security**

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- The Port estimates the cost of cards and associated readers, per employee, to be US\$132.50. The price will vary from port to port.
- Casual and day workers are a problem. The cost is too high to pay for workers who only work during "busy seasons." The port has come up with a couple of scenarios that would mitigate cost for casual employees. No plan has been decided on yet.
- Another challenge that must be resolved is port access. The current regulations for identification only require you to have a business need and a government-issued ID to go into the port. This must be addressed, and standardized, if TWIC is going to become a widespread reality.

Resources

Transportation Security Administration (TSA)
www.tsa.gov

Homeland Security Presidential Directive 12
www.osec.doc.gov/osy/HSPD12/HSPD-12Information.htm

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Transportation operation centers and their role in homeland security

Moderator

LTC Joseph T. Booth
LSP Ret., Gulf Coast
Manager, Public Safety
and Homeland Security
Solutions, Commercial
State and Local Group,
Information Technology
Sector, Northrop Grumman

Panelists

Richard Steeg
Northern Virginia Regional
Operations Director,
Virginia Department
of Transportation

Paul Sullivan
Chief Liaison, Federal
Highway Administration
Emergency Transportation
Operations, U.S. DOT

Gene Donaldson
Traffic Management Center
Operations Manager,
Delaware Department
of Transportation

Regional transportation operation centers need to interact with each other and eventually roll the information into a federal entity. The centers would publish security trends by analyzing specific events and the panel discussed how to address security issues from an analytical perspective.

Highlights

- Federal Highway Administration does not own, operate or manage the roads. That is the individual state's obligation. The Federal Highway Administration only provides technical assistance, knowledge and tools as requested. Its main mission is in congestion mitigation.
- The Federal Highway Administration sees incident management as a continuum. It starts with the high probability traffic accidents that have low impacts, and moves on to low probability high impact disaster scenarios. It believes that both ends of the continuum can be addressed by consistently using the same resources, the same people and the same tools and techniques.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- The U.S. DOT feels that all transportation operations personnel should read its pamphlet entitled "Simplified Guide to the Incident Command System for Transportation Professionals." It's not as important to professionals working in states that do a lot of evacuations, such as hurricane states.
- On the Federal Highway Information system Web site, there are specific publications based on lessons learned. There are 26 documents on best practices in the use of transportation operations centers in an emergency. And there are over 200 documents on traffic incident management. There are documents on transit security, aviation security and highway security. It is a secure site. If you have a .gov address or you are a vendor that works for a government entity, you will be allowed access with a password to that site.
- Most states should, or need to, operate a 24x7x365 center and are involved with incident management on a day-to-day basis. These day-to-day operations should form the basis of incident management.
- The Delaware Emergency Operations Plan falls under Delaware Emergency Management Agency (DEMA) and it created a Delaware transportation security plan.
- What Delaware is focused on, right now, is to move everyone to the same radio system, an 800 MHz radio system. Currently Delaware is working Pennsylvania, Maryland, New Jersey and New York on how to integrate our systems. The plan is to be directly connected from basically the DC area to New York City by next year.
- Transportation management needs to incorporate resource sharing. With roads to be controlled, communication and coordination needs to be developed at a regional level, there should be a focused effort to identify and categorize available resources. A problem at an interchange in one state can impact traffic over an entire region.
- Transportation had an increasing role in emergency incident management. This has led to the creation of an entity that is currently being planned and developed in the National Capital Region called MATOP (Metropolitan Area Transportation Operations Coordination Program). It is intended to be a virtual traffic management function or center. The idea is that the partners all have 24x7x365 operating centers and in some protocol yet to be determined, there is very likely to be a rotating regional desk with its own set of operating procedures, management protocol and dedicated resources.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- The best model today is Houston TranStar. TranStar was created in 1993 and Texas thought ahead; it wanted the emergency management and transportation management together. The state of Texas, the Texas Department of Transportation Harris County, the Metropolitan Transit Authority and the city of Houston, all have representation at Houston TranStar.
- Houston TranStar, a national leader in freeway incident management, uses state-of-the-art technologies to reduce congestion on major roadways. Monitoring traffic incidents with more than 600 regional closed circuit television cameras (CCTVs), staff at the TranStar center dispatch vehicles to remove debris or hazardous materials, communicate with emergency vehicles about the most direct routes to an accident scene, and send tow trucks to stalled vehicles.

Resources

Houston TranStar
www.houstontranstar.org/about_transtar/

Federal Highway Administration
www.fhwa.dot.gov/index.html

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Critical infrastructure protection

- ▶ Protecting your critical infrastructure program info
- ▶ Federal initiatives in the chemical threat area
- ▶ Cyber protection
- ▶ Follow up to October Pennsylvania Regional CIP Workshop
- ▶ CIP from a private sector perspective

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Protecting your critical infrastructure program info

Moderator

Richard Driggers
Director, ACAMS, DHS

Panelists

Harvey Eisenberg
Assistant U.S. Attorney;
Chief, National Security;
Coordinator, Anti-Terrorism
Advisory Council, District
of Maryland

Mike McAllister
Deputy State Director,
Security & Emergency
Management,
Virginia Department
of Transportation

Constance McGeorge
Special Assistant, Virginia
Office of Commonwealth
Preparedness

The development of effective plans to protect critical infrastructure (CI) depends heavily on identifying and assessing the vulnerability of CI assets, the vast majority of which are owned and operated by the private sector. Because of the sensitive nature of information about these assets from both a physical vulnerability standpoint and an economic competitiveness standpoint (i.e., desire on the part of the private businesses to not let competitors know too much about their assets), there are numerous issues surrounding the sharing of this information. These include statutory limitations at the state level and reticence on the part of the private sector to participate in any program that involves access to closely held information.

The Automated Critical Asset Management System (ACAMS) is a Web-based platform and tool set for the recording and sharing of CI information. It is in widespread, though not universal, use at present, and is the platform that has been adopted by DHS. When combined with the provisions of the Protected Critical Infrastructure Information (PCII) program, ACAMS can provide not only needed access to CI information, but assurances that the information is accessible only by those with a need to know.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Highlights

- ACAMS was initially developed by the Los Angeles Police Department as part of Operation Archangel, an initiative to identify and protect critical infrastructure and key resources in the Los Angeles metropolitan area. It has since been taken over by DHS.
 - ACAMS is designed to be used by local first responders and emergency managers. These are the individuals who populate the ACAMS database. PClI-trained and certified private sector organizations can also submit information to ACAMS on a voluntary basis. ACAMS relies heavily on local involvement and public/private partnerships.
 - The capabilities of ACAMS are continuously evolving and now include the integration of open-source data (e.g., ACAMS information was merged with data about the 2007 California wildfires to assess which CI assets might be affected).
 - ACAMS supports Homeland Security Presidential Directives 7 and 8, and use of it ensures that state, local and regional CIP programs are consistent with the National Infrastructure Protection Plan (NIPP). An important value of ACAMS is that it provides a common, consistent platform, taxonomy and tool set for CI information management and analysis.
 - Training is an important part of ACAMS, to ensure accurate and consistent vulnerability assessments and quality of data.
- DHS is working to encourage wider acceptance of ACAMS nationwide, but is not mandating it because different states have different needs. ACAMS is one answer, but not the only answer. The wider the acceptance of ACAMS, the more effective it can be.
 - 13 states currently have data loaded into ACAMS, with information on 20,000 assets.
 - 36 states are approved for PClI access.
 - There are 1,143 users of ACAMS nationwide.
- Protected Critical Infrastructure Information is an information-protection program that enhances information sharing between the private sector and the government. If the information submitted satisfies the requirements of the Critical Infrastructure Information Act of 2002, it is protected from the Freedom of Information Act (FOIA), state and local disclosure laws, and use in civil litigation. PClI cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements.
 - PClI enables controlled, two-way information sharing between government and the private sector.
 - Access to PClI information requires authorized user training, non-disclosure agreements, homeland security duties and need to know. This results in state accreditation.
 - PClI is one way in which private sector organizations can be assured that their sensitive information is protected.
 - It is up to the states to implement appropriate access rules; PClI provides a framework.
 - Private organizations that input data into ACAMS under PClI can see their own information, but not necessarily that of other companies.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Interdependency between affected critical infrastructure assets is an important sticking point when determining who gets access to CIP information. For example, a chemical plume might cross state lines, or a hurricane might take out key assets that have a downstream effect on other states.
- ACAMS and PCII can be effective tools for needed information sharing, but a combination of the need to tightly control information and statutory limitations hampers this initiative. This is the primary reason why there isn't more widespread information sharing more than six years after 9/11.

Resources

ACAMS information

www.dhs.gov/xinfoshare/programs/gc_1190729724456.shtm

Protected Critical Infrastructure Information program

www.dhs.gov/xinfoshare/programs/editorial_0404.shtm

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Cyber protection

Moderator

Dennis Dworkowski
First Vice President,
InfraGard

Panelists

Sheri Donahue
Managing Director,
InfraGard National
Members Alliance

Harvey Eisenberg
Assistant U.S. Attorney;
Chief, National Security;
Coordinator, Anti-Terrorism
Advisory Council, District
of Maryland

Jaime Chanaga
CISSP, CISA, Vice-President,
Enterprise Architecture,
CA, Inc.

Because of the increasing importance of information technology and data communications to the global economy, cyber protection has assumed great importance. It is likely that any potential major terrorist attack on the United States will include a significant cyber component, not only to cause direct economic and social damage, but also to disrupt recovery efforts.

This session touched briefly on the issue of cyber-protection in general.

- Businesses are much more difficult to protect today than they were a few years ago, because of increasing reliance on IT and data communications.
- The greatest return on investment in cyber security is in people, not technology. Firewalls and other technological solutions are useless if personnel do not practice effective security measures.
- Protection is a “three legged stool.” Physical protection, access to information (rules-based) and personnel.
 - There will always be some information that will get out because it’s impossible to hide.
 - The greatest effort should be expended to protect the most important information and resources.
 - To get buy-in from your organization, it is necessary to establish the value of training and personnel-centric security. Identifying and quantifying risk is one effective way to do this.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- There needs to be more integration and dialogue between the private sector and government regarding cyber protection.

The bulk of the session described InfraGard, a program designed to foster information and expertise sharing between the private and public sectors, with an emphasis on cyber security.

- InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. It expanded nationwide and was soon associated with the National Infrastructure Protection Center (NIPC), which is now run by DHS. The FBI retained InfraGard as an FBI-sponsored program.
- InfraGard is primarily a networking organization that fosters the creation of personal contact and relationships, and the passing of information. It affiliates local owners and operators of critical infrastructure with the federal government. It is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants. InfraGard membership is free, but does involve a records check.

- The primary purpose is the dissemination of subject matter expertise and information of interest. For example:
 - The FBI can call on InfraGard members to become educated about technical matters that may help in the course of investigations, or to solicit needed intelligence.
 - InfraGard members can become aware of best practices being employed by other members through direct contact.
 - Members can be made aware of useful programs that they might not otherwise hear about.
 - One of the panel members emphasized the need for public involvement in homeland security, noting that the media has not done a good job of passing along information about the ongoing threat. InfraGard can help to bypass this issue by, in some cases, giving members advance notice of important events such as impending threats that have not reached the mainstream media.
- There are 86 InfraGard chapters with a total of some 20,000 members, geographically linked with FBI Field Office territories. Each InfraGard chapter has an FBI Special Agent Coordinator assigned to it. The private sector's side of each chapter is a separate, not-for-profit organization called the InfraGard Members Alliance. In practical terms this means that while the FBI sponsors the program, the members can also interact with other federal agencies and organizations through memoranda of understanding (MOUs).

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

–The DHS has instituted a cadre of Protective Security Advisors (PSA), tasked with connecting to local authorities and private sector organizations, in an effort separate from the established InfraGard program. Through a collaborative effort, PSAs were made members of InfraGard, thus leveraging an existing organization to facilitate their work. PSA involvement with local InfraGard chapters also provides a pipeline back to DHS for private sector InfraGard members.

–Parallel organizations, such as the government- and law-enforcement-focused Anti-Terrorism Advisory Councils (ATACs) can use InfraGard as a resource to reach out to the private sector, and vice-versa.

- InfraGard chapter governance is left to the individual chapters, so as to create a better fit with varying local needs. For example, a chapter in an area with a large transportation sector might have greater TSA involvement than a chapter in a primarily agricultural region.
- Chapters have regular meetings, monthly or sometimes quarterly. This further facilitates information sharing among chapter members who might not otherwise be in contact with one another.

Resources

InfraGard home page (overall program)
www.infragard.net/

InfraGard Members' Alliance (member side)
infragardmembers.org/

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

CIP from a private sector perspective

Moderator

Ian Hay
President, SouthEast
Emergency Response
Network (SEERN)

Panelists

Mike McAllister
State Security Director,
Virginia Department
of Transportation

Roisin McCaffery
Assistant Director,
Pennsylvania Office of
Homeland Security

Jim Montagnino
CEO/President, The
National Center (NC4)

Matt Foosaner
MA, CBCP, CHS-III, Sprint,
Director, Emergency
Response Team

Private industry built and owns 85-90 percent of the critical infrastructure in this nation. The business community and the public sector approach CIP from varying viewpoints and different levels of expertise and resources. Because of the commonality in safety, security and economic well-being, private and public sector must forge a workable alliance in emergency preparedness.

Highlights

- The mission of SouthEast Emergency Response Network (SEERN) is to foster a true public and private and academic partnership, ideally connecting to the one common operating picture – communicating in real time and creating a sustainable regional process of collaboration and information sharing.
- If private industry doesn't protect its critical infrastructure, paychecks don't show up, and that failure will drastically impact our lives.
- The moderator noted that we have to stop preparing for the last disaster, and become prepared with an all hazards approach to any disaster.
- Fusion centers have the potential to become a logical nexus for an all hazards approach.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Specific regional threats need to be addressed by the private sector as well. For instance, in the Southeast, it is specifically the New Madrid fault, which runs along the line of Indiana, Tennessee, and Missouri. When this fault cracked in 1911, it rang church bells in Boston. It could displace 1.5 million people, which is Katrina and a half. We need to take this fault seriously especially because UPS and FedEx, as well as transportation hubs, are right in that area.
- Virginia has embraced the National Infrastructure Protection Plan (NIPP) in the state's approach to critical infrastructure.
- To attempt to protect everything means to protect nothing and so we have to make some tough decisions regarding what is critical infrastructure (CI) and what are key resources (KR). Virginia uses the framework established in the Homeland Security Presidential Directive 7-HSPD7.
- Constellation Automated Critical Asset Management System (ACAMS), a free system that DHS has developed, enables the flow of information between the public sector and the private sector. Government and private sector will actually be able to share information, securely and protected through a program called Protected Critical Infrastructure Information (PCII). It provides a set of tools and resources that help law enforcement, public safety and emergency response personnel:
 - Collect and use CI/KR asset data,
 - Assess CI/KR asset vulnerabilities,
 - Develop all-hazards incident response and recovery plans, and
 - Build public/private partnerships
- Pennsylvania follows the Commonwealth Critical Infrastructure Protection Program. It is tied in with the NIPP, but at a state level, and it encompasses all CI/KR and significant special events not just at the federal level, but in regards to all the different players who are working to collect all the information.
- As a critical infrastructure provider, Sprint Nextel has responded to 26 presidentially declared disasters in five years and participated in over 120 training exercises and national special security events. The company supports communication packages for virtually every agency at a state, local and federal level in law enforcement, fire, EMS and the military.
- There are only two sectors that are actually linked in a symbiotic relationship to every other sector: power and telecommunications; because without those, you are not going to run other systems.
- Eighty-five percent of government infrastructure information technology is run by the private sector.
- Keywords in this session, as pointed out by the moderator, were: relationships, communications, partners, interdependencies. All of which must be fostered between government and the private sector in order to protect CI/KR.
- Panelists agreed that working together, sharing information and running exercises outlining how information is shared whenever an event occurs – be it a natural or a man made disaster – are key in protecting CI/KR.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Apathy and bureaucracy are major stumbling blocks.
- Although interoperable communications systems are desirable in an incident, no "100 percent bulletproof" system exists.

Resources

National Infrastructure Protection
www.dhs.gov/xprevprot/programs/editorial_0827.shtm

Request for fusion center white paper
www.rsvpbook.com/event.php?408404

Homeland Security Presidential Directive 7
www.fas.org/irp/offdocs/nspd/hspd-7.html

Constellation ACAMS
www.dhs.gov/xinfoshare/programs/gc_1190729724456.shtm

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Federal initiatives in the chemical threat area

Moderator

Kevin Daniel
U.S. EPA Region-III,
Office of Enforcement,
Hazardous Site Cleanup
Division, Oil and Prevention
Branch, RMP Chemical
Enforcement, EPA

Panelists

Charles Caulley
Department of
Homeland Security
Infrastructure Protection,
Chemical Security
Compliance Division

Glen Rudner
Hazardous Materials
Officer, Region 1,
Virginia Department of
Emergency Management

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) was developed to assist in product design to help inform infrastructure owners and operators of any threats they may potentially face, as well as to better inform their security planning and investment decisions. The Chemical Facility Anti-Terrorism Standards (CFATS), Interim Final Rule went into effect June 8, 2007.

Highlights

- In Virginia, they began really thinking about chemical threats after the 1984 incident in Bopal, India. In Northern Virginia there has been tremendous outgrowth of chemical facilities that are of great concern to the local population.
- In 1985, the commonwealth undertook the responsibility of studying hazardous materials training response and planning, and the decision was made that the Virginia Department of Emergency Services, now Emergency Management, would be the leading agency for all hazardous materials response and provide hazardous materials response capabilities to the localities throughout the commonwealth.
- In 1987 through 1988 Virginia worked with all of its 143 localities and had them sign memorandums of understanding (MOU) that they would be able to provide certain capabilities within their localities. After that the commonwealth will then rely on individual regions and regional

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

response to maintain chemical response capabilities. At the same time, industrial facilities themselves put up and set brigades and hazardous materials response teams on sites. In 1988, 13 teams were established.

- The basic Virginia plan is very simple, and provides for response and recovery that is comprehensive and covers all the points laid out in the framework set forth by FEMA, the EPA and all of the other federal agencies that have asked the states to use their framework and model for Emergency Operations Planning.
- In Virginia, the state requires that local governments be responsible for identifying their incidents, reporting the incidents, identifying the hazard and the initial response.
- Once a locality exceeds their resources they will request assistance from the state through the Emergency Operations Center. Once the emergency is declared, it goes to the Governor's office and the Governor makes the declaration from the state perspective. In the meantime, aid is going to the local government through all the state agencies. After that, Virginia waits for the President to declare an emergency and DHS and FEMA to do their job and hopefully the assets will be coming from the federal government.
- Department of Emergency Service tasks each of the localities to have an Local Emergency Planning Committee (LEPC). Each locality should have an Emergency Coordinator, and he/she should appoint a Hazardous Materials Coordinator. Usually, in the localities, the Hazardous Materials Coordinator will work with the fire chief, and LEPC chairman is normally a local industry leader.
- In April of 2007 the Department of Homeland Security issued the Chemical Facility Anti-Terrorism Standards, authorizing under Section 550 under the Department of Homeland Security Appropriations Act of 2007 directing the Department to identify, assess and insure security at high-risk chemical facilities.
- In those standards is Appendix A, which lists over 200 chemicals of interest. The appendix provides a screening threshold quantity for those chemicals.
- Once Appendix A becomes finalized and is published, your facility has sixty days to fill out certain forms and submit your information to DHS.
- There are some exceptions: public water systems, any facilities owned and operated by DOD or DOE, any NRC Regulatory, any federal water pollution control. If you ship or receive anything through your waterway, you're covered under MTS, the Maritime Transportation Act. These are the exceptions.

Resources

Virginia Department of Emergency Management
www.vdem.state.va.us/

EPA Hazardous Site Cleanup Division
www.epa.gov/reg3hwmd/

Chemical Facility Anti-Terrorism Standards
www.dhs.gov/xprevprot/laws/gc_1166796969417.shtm

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Follow up to October Pennsylvania Regional CIP Workshop

Moderator

Roland R. "Bud" Mertz
PA, Deputy Director for
Infrastructure and
Community Liaison,
Pennsylvania

Panelists

Brian K. Wright
New York State Office of
Homeland Security

Mary D. Johnston
Homeland Security
Project Manager
Commonwealth of
Pennsylvania

Governor's Office
of Administration
Office for Information
Technology
Public Safety Community
of Practice

Steve Birnie
Strategy Implementation
Group, SC Law Enforcement
Division (SLED) for the
Homeland Security Advisor

This was a debriefing on the October Regional CIP Workshop hosted by the All Hazards Consortium in Pennsylvania.

The panel consisted of those who participated in the workshop and summarized and discussed the next steps as a result of the information gathered.

Highlights

- In October of 2007, representatives from the National Capital Region, Department of Homeland Security, Pennsylvania, Maryland, Virginia, Delaware, New Jersey, New York, Ohio, Kentucky, Tennessee, West Virginia and South Carolina met to discuss Critical Infrastructure Protection (CIP). This was the first of an annual series of CIP workshops designed to create a sustainable regional process of collaboration and information sharing.
- The goals of the October workshop were:
 - To have each state share information that relates to their CIP efforts to date, including challenges, lessons learned, best practices, private sector involvement, etc.
 - To further strengthen the CIP strategies within each state as well as the region
 - To identify regional, multi-state CIP efforts that may be funded or undertaken over the next several years
 - To capture and document the above into a regional white paper that provides an executive summary with regional consensus recommendations and next steps

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

**Critical infrastructure
protection**

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Interoperability was identified as a major stumbling point. It was found that states, private industry and federal entities need to agree on and possess a standard set of technology tools to facilitate information sharing and interoperability. Panelists recognized the benefit of Protected Critical Infrastructure Information (PCII) accreditation when it comes to information sharing.
- Currently, states, localities and regional partners lack an interoperable software system and this means that efforts are potentially duplicated, information sharing is stunted and resources are not being maximized.
- The states also recognize the benefit of having information sharing protocols that limit the distribution of sensitive information on a need-to-know basis. Rules also need to be developed and implemented around interoperability and information sharing. Some outstanding issues are: how do states exchange information? Who can see what, and why can they see it? How do you identify users? Further issues surround sharing classified and sensitive information.
- The solutions to many of the problems that states have uncovered in CIP are just now in development phase. Further, each state is at a different point in the development cycle. Finally, each state was working on different issues relative to development and implementation of the CIP programs.
- The overwhelming majority of the states that participated in the October meeting are relying on federal funds. All states are struggling due to the federally mandated 80-20 percentage of funding that should be spent on state vs. local levels.

Hence, states are investigating funding sources for statewide CIP initiatives.

- All attendees agreed that phase-phase interactions with the private sector should continue.
- The panelists also believe that they should promote regional intra- and interstate working groups and conferences, with sector-specific working groups in the state; information learned in those groups must be passed to the local jurisdiction and then to the regional level in their CIP program.
- The role of the fusion center must be refined. State and regional fusion centers can help insure that intelligence gathered all levels is integrated into the CIP management program.
- A regional white paper is still in the process of being developed and will be provided for review by the regional government working group members. The white paper will contain a synopsis of the workshop along with the regional recommendations provided by each of the states.

Resources

AHC October meeting agenda
www.ahcusa.org/documents/CIP%20Workshop%20Agenda.pdf

Request for fusion center white paper
www.rsvpbook.com/event.php?408404

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Emergency management

- ▶ Special needs populations evacuations
- ▶ Economic recovery from a major incident
- ▶ A Regional Perspective: National Incident Management System (NIMS) & NIMS-compliant Incident Command System Implementation
- ▶ New EOCs – opportunities and pitfalls to avoid
- ▶ Emergency management and gangs: What is the link?
- ▶ 3D virtual incident management training
- ▶ National Response Framework
- ▶ Regional continuity and catastrophic planning

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Special needs populations evacuations

Moderator

Christy Morris
Deputy Secretary for
Legislative Affairs,
West Virginia Department
of Military Affairs and
Public Safety

Panelists

Janice A. Holland
Associate Director/Clinical
Associate, Center for
Excellence in Disabilities

Trevor Rikken
Regional Red Cross Rep

Paul Fosdick
Technical Director, Northrop
Grumman Mission Systems

Laurel Radow
U.S. Department of
Transportation (DOT)

This panel discussed how definitions of “special needs” vary from state to state, and jurisdiction to jurisdiction. It also discusses how mass evacuation plans accommodate special needs populations, and how to make recommendations with regard to standard operating procedures in the event of a disaster.

Highlights

- After September 11, 2001 the Federal Highway Administration Office of Operations did a series of response/recovery workshops. It was determined that the local and state Department of Transportation personnel were essential to emergency response planning.
- People with disabilities comprised about 25 to 30 percent of those affected by hurricanes Katrina and Rita. Yet, panelists found that disabilities/special needs were not defined in a consistent manner across jurisdictions, which leads to confusion on which special needs populations need assistance during multi-jurisdictional emergency evacuations.
- For the Red Cross, during and after Hurricane Katrina, a lot of different issues arose around serving people with disabilities.
- One way to address issues may be a new target capabilities list (TCL) describing Functional and Medical Support Shelters.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- This sort of shelter would be something between a general population shelter and a federal medical station, where special needs people might get a little more assistance than from a general population shelter, such as a monitoring situation where they wouldn't necessarily need to be in a hospital but they need some nursing attendant.
- The TCL is still in draft form at the Department of Homeland Security.
- FEMA is also trying to put together a definition of special needs. The Red Cross isn't fully on board with it, as it contains categories like transportation-disadvantaged and limited English proficiency, which the Red Cross doesn't classify as special needs
- The Red Cross is developing a checklist for use at shelters to determine whether or not a person's special needs could be met at each particular shelter.
- Shelters should purchase medical cots: these cots have a higher weight limit and are higher off the ground; a lot of elderly people have difficulty getting off low-slung cots.
- Panelists were startled to find that some statistics show that 58 percent of people with disabilities do not know whom to contact about emergency plans for their community in the event of a disaster. Furthermore, 50 percent of persons with disabilities were employed full-time or part-time, and say no plans have been made for a safe evacuation at the local level.
- In West Virginia, they have addressed how to best get emergency medical equipment in place during evacuations, and how to get to the special needs people in order to evacuate them. This planning involved locating special needs people and identifying who would pick those people up.
- One problem mentioned was that you don't want the drivers evacuating ahead of when you want them to be picking up special needs people. So drivers need to be dedicated, and they need to be located in proximity to where they're needed. States have to include that into the modeling.
- Involve the postal service in your planning, as they know where everybody is, and pretty much after they deliver your mail on a daily basis, they usually know who the special needs people are. Also, local fire departments usually know where special needs people live.
- West Virginia has alerted its citizens that they need to plan to be self-sufficient for seventy-two hours or more.

Resources

National Incident Management System
www.fema.gov/emergency/nims/index.shtm

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Economic recovery from a major incident

Moderator

Kim Fletcher
Beck Disaster Recovery

Panelists

Jeremy Scheinker
State COOP/COG
Program Manager,
Maryland Emergency
Management Agency

Joan Grewe
TerreStar Networks Inc.

Matthew Greenwald
Government Relations
Officer for Homeland
Security, Washington
Metropolitan Transit
Authority

As many as 80 percent of businesses close within 18 months of a major incident, and up to 90 percent of those that lose data as the result of an incident close down within two years. On the public side, the loss of tax base has a major impact on the ability of local government to provide services. For this reason, planning for recovery is critical.

The session dealt with disaster recovery planning from three different perspectives: state and municipal governments and the private sector. Viability was a core focus. Planning must take into account interdependencies, limited resources and a wide range of possible disasters.

Highlights

- The panelists emphasized the need for flexible planning that can provide continuity of operations (COOP) regardless of the severity and nature of the disaster, whether it's highly localized (affecting a single building) or regional in nature.
- Identification in advance of critical functions and the personnel needed to accomplish them is necessary. Other functions can be given lower priority and brought back online over time. A critical function was defined as something that may need to take place at least once in a two-week span.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Because of the different needs of different sectors, there is no “one-size-fits-all” plan, though there are common elements, and in many areas industry standards have been established. A wide variety of planning tools and resources have been put in place by state and federal agencies.
- Economic modeling (i.e., identifying the specific impact of disaster on various parts of the economy) can be an important tool in determining how to construct a recovery plan for best effect.
- COOP and COG (Continuity of Government) plans have been in place for many years, but have only been mandated recently. Not all government agencies have COOP plans in place, but there is a strong trend toward implementation.
- Family support is essential to successful recovery, because individuals will always place a much greater priority on ensuring the safety of their families than on returning to work.
- Personnel who are not needed for critical functions still play a valuable role, providing support (e.g., child care) for those who tend to critical functions.
- The intelligent use of available financial resources is an issue. Unfunded plans have little or no chance of success. The panelists recommended looking for opportunities to cooperate with other businesses and agencies on a memorandum of understanding (MOU) basis. Also, there are risk assessment resources available to help identify the most critical items to be addressed by continuity and recovery planning.
- Coordination with partners and vendors when planning for recovery is important, because their input of goods and services may directly affect the viability of a given organization’s recovery efforts.
- Effective recovery and continuity planning can help mitigate the severity of a disaster. The example cited involved the 2007 California wildfires. Los Angeles County had a better plan in place than did San Diego County, so the impact was reduced.
- Plans must account for dependencies and interdependencies. Two examples were cited: the city of Cleveland, where all water must be pumped from the lake, has a critical dependency on the availability of electricity to pump the water. In Washington, DC, the 700,000-plus rail system riders would have to find alternate transportation should the metro system go out of service, which would severely impact the highway system.
- Government and private sector organizations can and should collaborate on ongoing problems. The example cited was the continuing drought in Georgia; the government has issued an RFI to private industry, asking what they can do to help mitigate the situation.
- A new development on the private sector side is the establishment of Business Operations Centers, which mirror and interface with state Emergency Operations Centers. A key aspect of this is the neutrality of the private sector operations center, so there is no assumption of sales or creating contracts merely through interaction.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Restoration of confidence is an important element of recovery planning. Getting displaced workers and residents back into the area, going to work and using public facilities is vital to fast recovery. This has been a key issue in the recovery from Katrina. Tax incentives and other forms of public assistance can be a key component to restoring confidence.
- The federal government can provide guidance on developing continuity and recovery plans, but it is ultimately up to individual organizations to set up and execute these plans for themselves, using their own resources as much as possible. Federal authorities cannot be relied upon to handle the entire load.

Resources

FEMA
www.fema.gov/

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

A Regional Perspective: National Incident Management System (NIMS) & NIMS-compliant Incident Command System Implementation

Moderator

Al Fluman
NIMS Director, DHS

Panelists

Steve Grainer
NIMS Coordinator,
Virginia Department
of Fire Programs

Joseph Roberge
NIMS Coordinator,
Pennsylvania Emergency
Management Agency

William (Bill) Campbell
New York State
Emergency Management

State NIMS directors spoke on how they are implementing the new requirements. Highlights included examples of factors that impede the progress and how they have they overcome those obstacles to implementation.

Highlights

- The National Incident Management Systems Division is part of the Preparedness Directive of FEMA; formerly it was known as the NIMS Integration Center.
- The components of NIMS are:
 - Preparedness
 - Communications and information management
 - Resource management
 - Command of management.
- The revised NIMS document from FEMA is still in draft form. It should be released when the National Response Framework is finalized and released.
- The revised NIMS document is easier to read and understand, with improved graphics. It still works towards establishing a common incident management system across the nation. The new document considered approximately 5,500 comments nationwide during revisions.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- However, the new NIMS document is a work in progress, and interested personnel should expect it to change over time. For example, there were 77 separate and distinct versions of just the five-page, multi-agency coordination section in the document. FEMA just accepted the 78th version.
- In the new document FEMA emphasized the importance of Homeland Security Presidential Directives, especially Homeland Security Presidential Directive 8.
- Mutual aid agreements between states are recommended and their importance is stressed, as is testing those mutual aid agreements in drills and exercises. No single jurisdiction has all the resources it needs.
- Common operating systems and interoperability were also stressed. Primarily, the emphasis has been on the hardware and software components of the common operating picture. We have the Homeland Security Information Network, but more focus needs to be given to how data is gathered, how it needs to be tied to objectives, strategies and tactics used at the incident command level. Additionally, that information needs to flow from there to the emergency operation center and across all government agencies.
- A national credentialing system is being developed, and will be distributed to state and local governments in 2008 through the Emergency Management Assistance Compact (EMAC). Essentially, this system will identify skills needed for positions deemed necessary for large-scale events and the individuals who possess those skills.
- There have been a few changes in the revised NIMS document on Command and Management; many changes have been made in the Incident Command System (ICS) nomenclature.
- Pennsylvania, in 2006, sent out 13,000 CDs with NIMS information as well as a template for the NIMS implementation plan. They sent it to all the local jurisdictions and it was overwhelming for them, too much information.
- For 2007, Pennsylvania formed two workgroups, one to focus on state agencies and one to focus on local jurisdictions. The jurisdictions worked on it first, decided what would work on a regional, county and local level and then turned the NIMS information over to the state agencies. This seemed to work better.
- Some obstacles Pennsylvania faced were local and state laws regarding jurisdiction, and the fact that some localities either did not have appropriate computer technology or even Internet access.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Basically, all parties in Pennsylvania agreed that incidents will be handled by ICS and the governor's proclamation formally adopted NIMS and mandated the use of ICS at all incidents.
- In New York, people tend to forget that the majority of New York State is more rural than it is urban, but they must focus on both aspects.
- New York State has an All Hazards incident management team of state and local representatives consolidated and combined from all the different organizations. It has been a very effective process.
- New York believes it must focus more on multi-agency training programs, and combine the different disciplines involved in the training.

Resources

National Integration Center (NIC) Incident Management
Systems Integration Division
www.fema.gov/emergency/nims/

NIMS compliance and technical assistance
www.fema.gov/emergency/nims/nims_compliance.shtml

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

New EOCs – opportunities and pitfalls to avoid

Moderator

Michael A. Hughes
Northeast Business
Development Manager,
Commercial, State
and Local Group,
Northrop Grumman

Panelists

Harry E. Colestock III,
Director of Operations,
Virginia Department of
Emergency Management

Mark Marchbank
C.E.M., Deputy Coordinator,
City of Virginia Beach,
Fire Department/
Emergency Management

You can be certain that a well-designed Emergency Operation Center (EOC) can greatly benefit the coordination of response and recovery activities. Clear operating procedures, staff roles and responsibilities are required as is an effective workspace and a safe location.

Highlights

- When you begin to look at an EOC, you're dealing with a number of different organizations throughout your state and local government, including, but not limited to: police, fire, transportation, health and human services.
- Panelists recommend a visioning process when planning an EOC. This process has been adopted by the All Hazards Forum and Consortium and was followed in developing the most recent white papers for the fusion center, the inoperability workshop and the critical infrastructure protection workshop.
- In this process, a municipality would document "as is" and "to be" EOC processes and develop a framework for moving forward. It is recommended to facilitators and subject matter experts to help develop the high-level roadmap. The goal is to really develop a document and a methodology that will help you to go through the entire process from visioning statement, to statement of work, to an actual EOC.
- It is advisable to plan goals for an EOC in one-, five- and 20-year increments.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- When planning, match participants, competencies, personnel and strategies developed along the way; plan to participate in conferences and events; and take advantage of opportunities to do site visits to understand how other localities have gone about establishing and building new EOCs.
- Basic questions must be addressed in planning an EOC, such as:
 - Current and future needs
 - Operational needs of the staff
 - Budget and space limitations
 - Time restraints
- Panelists noted that time spent in the planning process for an EOC would be invaluable later, for example, to establish a construction specification list.
- One major part of the design of an EOC is to make it a technological focal point; data sharing capabilities and data interoperability are major issues.
- Separate, secured and self-sufficient LAN connections that will allow computers to survive and work when there is no power are key.
- In emergency management at this time, there is the new issue of National Incident Management System (NIMS) and how to make an EOC compatible or compliant in terms of NIMS using the Incident Command System (ICS) structure. Municipalities are experiencing a lot of ambiguity and inconsistency in the NIMS document in seeking to achieve compliance.
- An EOC that has connectivity and projecting capabilities will do well in terms of creating situational assessments. Using the Internet to make sure everybody is aware what's going on is a great asset for an EOC. Interoperability or integrated systems are very important.
- An EOC must be built and placed with regards to security, with threats considered ranging from drive-up bombers to simply providing a well-lit parking area for workers.
- Total costs for panelists' EOCs ranged from US\$10 million to US\$59 million.
- When an EOC is completed, panelist urged that localities make sure everything is fully functional before any workers are moved, because "When you're in you really are in." One panelist advised that EOC managers should:
 - Ensure contractor makes it right before you take possession.
 - Ensure handoff briefings are completed with all the players.
 - Understand how your facility works.

Resources

Eleven NFPA Standards for Emergency Responders
www.nimsonline.com/

Jacksonville, FL EOC NIMS
www.floridadisaster.org/CIEM/

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Emergency management and gangs: What is the link?

Moderator

Mel Blizzard
Director, Metropolitan
Washington, DC Fusion
Center; Commander,
JTTF and Synchronized
Operations Command

Panelists

Benjamin Johnson
Director of
Emergency Management,
City of Richmond

Sergeant Dennis Dudley
Frederick, Maryland
Police Department

Marilyn Di Paolo
Community Intervention
and Gang Program
Manager, Virginia
Department of
Juvenile Justice

Sheltering becomes problematic with gang involvement, both in sheltering rival gangs within the same facility and with gangs selling supplies illicitly within the shelters. The prevalence of gangs is widespread, even within the most rural areas. How does their presence affect response?

Highlights

- In 1975, the U.S. had approximately 81,000 gang members and 2,700 gangs. Today, we are looking at somewhere around 731,000 gang members and 21,000 or so gangs. All of the expert researchers in the field believe that this is really a gross underestimation of the number of gangs for a variety of reasons. Members are usually between 12 and 24 years old, although the average age is growing in both directions.
- A result of emergencies is a breakdown of normal organization and structure: Gangs have a structure and organization, and are willing to fill the void. With law enforcement stretched thin during an incident, gangs may see this as an opportunity.
- Anticipated gang-related problems during incidents are:
 - Interfere with recovery efforts
 - Disruptive in shelters
 - Potential criminal activity in shelters
 - Crimes against persons in and out of shelters

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Among the jurisdictions that report having gangs, 95 percent report them in high schools and 91 percent in intermediate schools.
- According to the National Youth Gang Center survey, in the U.S., gang membership is 49 percent Hispanic, 34 percent African-American, 10 percent Caucasian-White, 6 percent Asian. Most are well-armed.
- Check for gang membership in your community. Some signs are graffiti, crossed-out graffiti, hand signs, groups of young people dressed alike. You must identify gangs in your area. Knowing which gangs are in your community, and which gangs have a history of conflict, can greatly reduce problems when a sheltering incident occurs.
- In planning, ensure that you have provided for non-police security at shelters, and training for shelter workers to assist them in gang identification, what suspicious activity is and when to call police.
- Even if you have identified gang membership in your community, in an evacuation situation you must identify which community has evacuated to your shelters, and then ascertain the level of gang membership and/or rivalries and conflicts that are present in the evacuated community.
- Gang membership must be evaluated and prepared for during an emergency. After Hurricane Katrina, police and rescue personnel were fired on during rescue operations, mobile kitchens had food stolen by organized groups and there was looting in evacuated areas. All of this activity stopped when the National Guard showed up. However, there appeared to be no gang-specific problem in the shelters during Hurricane Katrina.
- If you identify potential troublemakers before they get to the shelters, or put separate gangs into different shelters, you may avoid problems.
- One panelist talked about an evacuation in Arizona, where gangs where sheltered with the general population. The gang members did not want to go to sleep when everybody in the shelter went to sleep, they were loud and disruptive. The police Gang Intelligence Unit entered the shelter and gave the gang members options: "You can go out at night and not stay in this shelter and we will provide you food, but you are not going to disrupt the rest of this shelter. We are not going to deny you any service. If you want the service, you stay here and you do not be disruptive, or you come here and pick up your meals." This was a planned response during evacuations.

Resources

Virginia Child Protection newsletter focusing on gang prevention
psychweb.cisat.jmu.edu/graysojh

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

3D virtual incident management training

Moderator

Michael Pack
Lab Manager, RITIS Project
Manager, University of
Maryland Center for
Advanced Transportation
Technology Lab

Panelists

John Burwell
Vice President,
Business Development,
Forterra Systems Inc.

Alvin Marquest
Maryland State Highway
Administration

Steve Austin
Emergency Responders
Safety Institute

Lieutenant Mark Henry
Maryland Transportation
Authority Police Force

This was a preview of an online, interactive first responder training game being developed for the I-95 Corridor Coalition. There was a live demo with responders from around the country, and audience members had a chance to participate and provide feedback on the development process.

Highlights

- The National Traffic Incident Management Coalition (NTIMC) is a coalition of organizations that represent 16 traffic incident management responder organizations. The I-95 Corridor Coalition, represented on the panel, is one of the members.
- The NTIMC has announced the National Unified Goal (NUG) for traffic incidents. The NUG is being implemented through state, regional and local traffic incident management partnerships.
- NTIMC and its partners at the national level are working together to provide tools and guidance to assist traffic incident management partnerships in implementing NUG strategies.
- The National Unified Goal outlines 18 strategies to meet its three objectives:
 - Responder's safety
 - Safe, quick clearance
 - Prompt, reliable communications

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Current training for first responders to traffic incidents can be very expensive, time consuming, requires travel and can be difficult to coordinate.
- The two main types of training programs for the first responder community are tabletop exercises, or full-scale scenarios that are played out in the middle of a field.
- Developed with the same tools used in the serious gaming genre, there are now online multiplayer training exercises available. These online exercises are realistic, engaging and easily scalable; the exercises can simulate something as small as a fender bender on the side of the road to a 20 tractor-trailer fire explosion.
- The training game discussed on the panel that is being developing is based on Forterra's OLIVE platform. OLIVE stands for the On-Line Interactive Virtual Environment. It's basically a game engine that has been designed to be easily reprogrammable.
- The U.S. military has invested approximately \$50 million in OLIVE.
- The panelists demonstrated the traffic incident simulation from Forterra Systems. Players were located in Louisiana, College Park, Maryland, and on-site at the All Hazards Forum.
- Forterra Systems software and services enable organizations to train, plan, rehearse and collaborate. Using industry-standard PCs, users generate realistic, collaborative, 3D simulations that scale from single user applications to large-scale environments with thousands of concurrent users.

- Some attendees thought that the simulation lacked the realism or reaction times of popular video games. Forterra's spokesman pointed out that in some popular games, the characters move two to three times faster than is possible in real-life. The company sought to replicate reality, so that you turn at the right, proper pace. If you change variables and make characters turn a lot faster, you get into potentials of negative training.
- Forterra's spokesman used the game Doom as an example: "When you're running around in the rooms, the hallways are about two to three times wider than they are in the real world, so it's really easy to run around and be able to see things and get situational awareness which is important just before you get shot. But in the real world, it's fairly narrow, and so if you have a rifle and you're running down a hallway and then you try to turn around, the chances of you bumping into the wall are very high." Because Forterra made this technology actually replicate real world conditions, it may seem a little bit boring to gamers.

Resources

The National Traffic Incident Management Coalition
timcoalition.org

National Unified Goal
www.transportation.org/sites/ntimc/docs/NUG%20Unified%20Goal-Nov07.pdf

Forterra Systems
www.forterrainc.com

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

National Response Framework

Moderator

Chris Geldart
Director of the Office of
National Capital Region
Coordination, FEMA

Panelists

Greg Cade
Assistant Administrator,
U.S. Fire Administration,
FEMA

John Droneburg
Director, Maryland
Emergency Management
Agency

On September 10, 2007, the Department of Homeland Security (DHS) released the draft National Response Framework (NRF), successor to the National Response Plan. The framework, which focuses on response and short-term recovery, articulates the doctrine, principles and architecture by which our nation prepares for and responds to all-hazard disasters across all levels of government and all sectors of communities. DHS is responsive to repeated federal, state and local requests for a streamlined document that is shorter, less bureaucratic and more user-friendly.

Highlights

- The National Response Framework outlines the importance of setting a strong and unified response for America. The framework outlines the roles and responsibilities of each level of government, along with the private sector and non-governmental agencies.
- Roles are included that have always been acknowledged, but never fully integrated in past documents (no new roles have been created; this document reflects those that already exist).
- The purpose of the framework is to serve as our nation's guide for all hazard incident response.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- The framework builds on the concepts of the National Incident Management System (NIMS) and the ideas of flexibility and standardization. It emphasizes the importance of preparedness, communications and information management, resource management and the incident command system.
 - The base document of the framework is intended for government executives and senior elected, appointed officials who have a responsibility to provide effective incident response.
 - The secondary pieces are for the emergency management practitioners, and they explain the operating structures and tools that are at the disposal of emergency management that can be used by all first responders at all levels.
 - From a usability standpoint, the panelists who worked on the document thought it did make sense to hear from people at the local level, the state level and other national organizations; people who are actually going to use this document. There are more people at the local level who are going to use the document than at the federal level. Over 5,815 comments were considered.
 - One consideration in writing the framework was to make it useable – to have a document that's useful in the little incidents that are occurring in everybody's communities, but then, as those incidents begin to grow, it can be rolled out to a regional level, a county level, a state level and, ultimately, the federal level. The framework should not ask someone to go out and figure out a whole brand-new way of doing business, but rather to expand on daily activities.
- The NRF includes the core document, as well as the following supplemental documents that will provide more detailed information to assist practitioners in implementing the framework:
 - Emergency Support Function Annexes: groups federal resources and capabilities into the functional areas most frequently needed in a national response (e.g., transportation, firefighting, mass care).
 - Support Annexes: describes essential supporting aspects common to all incidents (e.g., financial management, volunteer and donations management, private sector coordination).
 - Incident Annexes: addresses the unique aspects of how we respond to seven broad categories or types of incidents (e.g., biological, nuclear/radiological, cyber, mass evacuation).
 - National Planning Scenarios: these are the 15 specific events defined by the National Preparedness Guidelines that are being used to develop more granular strategic guidance and operational plans for federal, state, community and private sector practitioners for each of the scenarios.
 - Strategic Guidance: defines the broad base national priorities and capabilities and supports the development of specific plans.
 - Playbooks: provides checklists to ensure coordinated response to the 15 specific, high-consequence threat scenarios for federal and state governments, communities and private sector partners.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- One panelist noted that, "Folks at the federal level may be a little bit naïve in thinking that we're going to write a playbook that's going to work the same way in every one of the 50 states. That just is not going to happen."
- Panelists urged the audience to review the Framework and comment, as stakeholder input is vital to ensure utility and accuracy.
 - Comments should be submitted to respective agency headquarters for consolidation and submittal.
 - Use the comment form and follow instructions provided by DHS, and submit comments electronically to fema-nrf@dhs.gov

Resources

National Response Framework
www.fema.gov/emergency/nrf/

Department of Homeland Security
www.dhs.gov/index.shtm

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Regional continuity and catastrophic planning

Moderator

Delilah Barton
Director of Homeland
Security Programs,
Beck Disaster Recovery

Panelists

Bob Fletcher
President, Readiness
Consulting Services

Jonathan Nguyen-Duy
Group Manager, Business
Continuity Services, Verizon.

Matt Greenwald
Government Relations
Officer for Homeland
Security, Washington
Metropolitan Area
Transit Authority

Tim Beres
Director of
Security Programs,
The CNA Corporation

Steve Kral
Acting Senior Policy
Advisor, District of
Columbia Homeland
Security Emergency
Management Agency

Gordon Aoyagi
Director of Montgomery
County Homeland Security

The National Capital Region (NCR) defined Regional Continuity in its 2007 Regional Hazard Identification and Risk Assessment (HIRA). The NCR HIRA is a strategic analysis of the hazards that have the potential to significantly impact regional continuity in the NCR. Regional Continuity is defined as "the steady state of continuity in the lives of individuals, families and communities, as well as the local, state and federal government services and leadership that support them. It is further comprised of the infrastructure sectors and systems owned and operated by a strong and resilient public and private sector."

Highlights

- Most panelists were involved in hazard identification and risk assessment for the National Capital Region. It was a unique project that looked at hazards and risks from the regional perspective, and not specifically a local perspective. Twenty-seven different jurisdictions were deemed to be part of the National Capital Region (NCR).
- Last year Admiral Thad Allen noted that the response to Hurricane Katrina was very different than the normal hazard response because of what he coined as the "loss of civil society."

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- When planning for regional continuity, it must first be determined what kind of hazards can produce regional consequences.
- Critical assets and region-specific threats must be identified.
- At the regional level, Verizon typically focuses on the regulatory issues and then the state and local for first responder and operational issues. However, there is a gap of understanding between large private sector companies in a region and their public sector counterparts.
- Very few companies understand at what point you declare a disaster, and how service providers maintain operations. One of the biggest weaknesses within continuity of operations is supply chains, and both regions and companies need to go beyond the first step of identifying vendors and see whether they have a continuity plan.
- Washington Metro, in preparing for regional continuity, put in place a significant chemical and biological detection capability. The transit authority coordinates very closely with regional first responders and has a 24/7 training facility that regional and national first responders have gone through, to give the first responder community a better familiarity of transit systems.
- In terms of recovery from an incident, especially biological, cleanup of a transit system is complicated. In partnership with the Department of Homeland Security Science and Tech and Lawrence Livermore Labs, Washington Metro hopes to take significant steps at looking at more of the nuts and bolts aspects of actually cleaning up the system. It would still be a significant challenge to restore service.
- Politics are local, and all emergencies are local. It is around that basic premise which you build response capability, which is why it is so important to have mutual aid and why it is so important for us to invest in standardization of equipment, so that we can, in fact, leverage regional resources.
- One group continuing to examine regional continuity is The Infrastructure Security Partnership (TISP). TISP, a public-private partnership, is promoting collaboration to improve the resilience of the nation's critical infrastructure against the adverse impacts of natural and man-made disasters. TISP members represent the design, construction, operation and maintenance communities; local, state and federal agencies; academe; and other related organizations, work together to develop and implement cost-effective solutions to enhance the resilience of the nation's critical infrastructure by leveraging their collective resources and expertise regarding natural and man-made disasters.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Resources

Beck Disaster Recovery
www.beckdr.com/

The Infrastructure Security Partnership
www.tisp.org

Washington Metropolitan Area Transit Authority
www.ncrnet.us/iepdclearinghouse

District of Columbia Homeland Security and Emergency
Management Agency
dcema.dc.gov/dcema/site/default.asp

Montgomery County Homeland Security
[www.montgomerycountymd.gov/mcgtmpl.asp?url=
/content/homelandsecurity/index.asp](http://www.montgomerycountymd.gov/mcgtmpl.asp?url=/content/homelandsecurity/index.asp)

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Grants and procurement

- ▶ FY 2008 Homeland Security Grant Programs: The pre-award process
- ▶ FY 2008 Homeland Security Grants Programs: Post-award management

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

FY 2008 Homeland Security Grant Programs: The pre-award process

Moderator

Julian D. Gilman
Preparedness Officer –
Texas and New Mexico,
U.S. Department of
Homeland Security/FEMA

Panelists

Steve Kral
Administrator for the
District of Columbia Office
of Homeland Security

Mark Nugent
President, SecureGrant
of America

Nancy Ann Baugher
Director, Office of
Grant Operations,
U.S. Department of
Homeland Security

Edith Davis
NIH Bethesda

Robin Brabham
Grants Analyst, Metro Police
Dept., Washington, DC

In fiscal year 2008, a total of US\$3.2 billion will be available for state and local preparedness expenditures, as well as assistance to firefighters. Of this amount, US\$2.2 billion is requested for DHS to fund grant, training and exercise programs under FEMA. In addition, in coordination with the state preparedness grant program, DHS will be co-administering the US\$1 billion Public Safety Interoperable Communications grant program in partnership with the Department of Commerce. This session covered who should make up the Grant Procurement Team, and the process for developing a strong, competitive proposal. Strategic planning, implementation considerations, financial and program management was also addressed.

Highlights

- In fiscal year 2008, the Department of Homeland Security (DHS) will award more than US\$3 billion in grants to states, territories, urban areas and transportation authorities under 14 programs to bolster national preparedness capabilities and protect critical infrastructure.
- These grant programs provide US\$376.3 million more than last year to enhance the nation's ability to prevent, protect against, respond to and recover from terrorist attacks, major

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

disasters and other emergencies. This includes the department's two largest grant programs: the Homeland Security Grant Program totaling US\$1.69 billion, and the Infrastructure Protection Program totaling US\$852.4 million.

- The department focuses on three funding priorities for FY 2008:
 - Measuring progress against the National Preparedness Guidelines
 - Strengthening preparedness planning
 - Strengthen IED prevention, protection and recovery
- Law enforcement activities will become part of both the State Homeland Security Program and Urban Areas Security Initiative programs, with a requirement to spend at least 25 percent of each award on these important prevention and protection activities.
- As a result of the Post Katrina Emergency Management Reform Act, the 10 FEMA regions will have an enhanced role in grant activities.
- The burden on grantees will be reduced as the Enhancement Plan portion of the application has been replaced by the State Preparedness Report.

- The department's risk methodology for the grants has been revised to reflect input from the 9/11 Act, including the use of Metropolitan Statistical Areas.
- The department is also releasing many grant programs on the same day, with the goal of getting application materials out to the eligible applicants approximately two weeks sooner than last year's timeline.

Resources

Grant guidance from DHS
www.ojp.usdoj.gov/odp/grants_programs.htm

Grant guidance from FEMA
www.fema.gov/government/grant/index.shtm

Fact Sheet: Fiscal Year 2008 Preparedness Grants
www.dhs.gov/xnews/releases/pr_1201882312614.shtm

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

FY 2008 Homeland Security Grants Programs: Post-award management

Moderator

Julian D. Gilman
Preparedness Officer
Texas and New Mexico,
U.S. Department of
Homeland Security/FEMA

Panelists

Steve Kral
Administrator for the
District of Columbia Office
of Homeland Security

Mark Nugent
President, SecureGrant
of America

Nancy Ann Baugher
Director, Office of
Grant Operations,
U.S. Department of
Homeland Security

This session dealt with the question of who should be on the grants management team (represent each of the grants management disciplines of policy, program and financial responsibilities), how they interact, how to drive results and compliance requirements. The team approach is proven to be critical to effective grants management to ensure jurisdictions can closely coordinate all aspects of their homeland security program.

Highlights

- On your grant management team, you must have a lead writer. This is key when reporting back on how you spent your award money. The lead writer does not have to understand operations, as one panelist who uses an assistant county attorney to write reports explains: "She doesn't know an ax from a fire engine, but she can read that proposal and see if it makes sense from a readability perspective. We have one person that reviews technical aspects of our reports, and then the lead writer make sure it is readable."
- If you're not following project management principles, panelists believe that you will struggle to procure funds and manage your timelines. You must follow strict project management principles in handling every grant.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- When a grant is awarded, it is essential to assign one lead person to keep all records of how each dollar of that grant is spent.
- Records are essential, as administrators can spend as much as 50 percent of their time in audits. You must meet compliance regulations, and you will get hung up if you can't show receipts for any individual product.
- However, different firms interpret the auditing regulations differently. Always request that any auditing firm that comes in to audit books has individual expertise in Homeland Security grants. If it doesn't, you're going to be spending weeks training those individuals on how to audit your files. If they don't understand the Approved Equipment List, it will be a disaster.
- For example, for a grant management team of 10, one project manager would specialize in IT. Project management teams should be assembled according to their functional expertise.
- If you're going to do a sub-grant to an individual local jurisdiction, you must have a project planned in house. That individual project must decrease vulnerabilities within your state, and must be applicable against one or many of the target capabilities of the DHS. Also, you must make sure that the local jurisdiction actually spends the funds. Because at the end of the day, DHS is going to ask you, "Have you spent your funds?" The only way you could show spending is that you've reimbursed that local jurisdiction for that product or deliverable so you have to show that it has been spent.
- You must make sure you have the leverage to reprogram funds or individual local jurisdictions will then be at risk for not abiding by their project plan. One panelist said that adding in multiple special conditions on individual grants allows the leverage needed internally to hold jurisdictions to products on the back-end. The panelist utilized special conditions because the sub-grants have to be signed off by the local city administrator, and in turn they're held liable for those dollars. This is reviewed monthly. The panelist advocated making jurisdictions spend the awards within two years, rather than the three years allowable.
- The DHS extends grants all the time. Things happen, delays occur, shortages occur. Especially on the purchase of equipment such as fire trucks and ambulances, as long as a local government official sends some evidence that they are having an issue with delivery, the DHS will work with them. And that's certainly a reason to get an extension on a grant. The DHS expects to see those kinds of things, and just needs to know what happened in advance. Local governments, in particular, need to watch that.

Resources

Office of Grant Operations, U.S. Department of Homeland Security
www.ojp.usdoj.gov/odp/grants_programs.htm

District of Columbia Homeland Security and Emergency Management Agency
dcema.dc.gov/dcema/site/default.asp

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Health and medical readiness

- ▶ Pandemic flu
community impact
- ▶ Regional burn care
- ▶ Multi-jurisdictional
preparedness with
food safety

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

**Health and medical
readiness**

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Pandemic flu community impact

Moderator

Jonathan Nguyen-Duy
Verizon Business,
Group Manager – Business
Continuity Services

Panelists

Robert Briggs
Homeland Security
Advisor, Delaware
Department of Safety and
Homeland Security

Mike Robinson
Director, Program
Advancement/Business
Development, Virginia
Modeling, Analysis and
Simulation Center, Old
Dominion University

Trevor Rikken
Regional Red Cross Rep

Dr. Jodi M. Kuhn
Homeland Security
Consultant, Serco, Inc.

What are the states' abilities to declare and enforce quarantine and isolation? Can campuses be used as quarantine sites? What are mitigation strategies when critical infrastructure is threatened?

Highlights

- In preparation for the event of a pandemic flu, the private sector needs to focus on business continuity plans in the event that 40 to 60 percent of staff will not or cannot go to work. Remote working strategies and “social distances” are the starting points. Retail establishments will not be able to maintain social distances.
- Remote working strategies raise question such as, does a business have bandwidth available to support 40 percent of a workforce working remotely?
- For businesses, there are four primary questions:
 - Will the telecom network work during a pandemic?
 - Are the commercial networks prepared for pandemic as well as other disasters?
 - What is the practical reality of telecommuting during a pandemic or other similar event?
 - And finally, is their business equipped with a proper communications network.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Businesses must investigate their telecommunications provider business continuity plan.
- Loss of key personnel becomes critical in terms of planning. An emergency autonomous decision-making process is the best way to overcome this factor.
- From a civic standpoint, Delaware has taken proactive measures: the state has a State Pandemic Influenza Plan and support plans, which include mass distribution of vaccines and antiviral medicine. Contagious disease containment and measurement plan along with a quick reference guide called "Pandemic Influenza Response and Personal Protective Equipment Guide" are all available through the state of Delaware Web site.
- Delaware is also working to increase individual hospital's three-day pharmaceutical caches of doxycycline and ciprofloxacin to 10 days, and hopefully longer in the future.
- The Red Cross believes that it will have a shortage of volunteers during a flu pandemic, due to illnesses, and is therefore in favor of education efforts well beforehand. Local chapters are at various stages of the planning/education process; some are well along, others are just finally starting out.
- At Old Dominion University in Virginia Modeling, Analysis and Simulation Center they are focusing on computer modeling and simulation to help communities plan for pandemics and business continuation.
- Air, land, sea transportation and traffic patterns are all modeled, including reports of congestion, and effects on travel speed. You can model incidents and accidents and how those affect the time that it takes to travel across an area, and the time for medical response.
- For hospitals, you can model the suitability of hospitals for different kinds of care, their individual capacities, the staffing on hand – reserved or available – their activity levels, patients' status, and search capacity.
- Old Dominion University believes that the old methods for disaster planning are ineffective, as "20 emergency managers" in a meeting cannot possibly consider all factors.
- The college has four models it can run. For example, the first one is called the Mass Casualty Mode; a very robust simulation that allows you to look at a number of different infectious diseases. There are over 50 infectious diseases that are in the simulation including the avian flu. The model allows you to predict and graph out curves of fatalities versus time or the number of susceptible infected or recovered patients against time. It can model major metropolitan areas to the individual person level.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- This is not a medical model; it's meant to train those who oversee the medical facilities so that they can properly adjust for care. It allows you to see the effects of mitigating incidence. For example, if you quarantine an area, how does that change the spread of infectious disease? If you inoculate people in advance, how would that change the statistics? If you inoculate people during the event, how does that change the infected rate? How beneficial would it be to isolate the area to impose travel restrictions? If you delay your response, how bad is it?

- In planning, you must involve all members of Voluntary Organizations Active in Disasters (VOAD). These non-profit organizations will be key in replacing/relieving/assisting sick personnel.

Resources

Delaware Pandemic Influenza Plan
www.dhss.delaware.gov/dph/files/depanfluplan.pdf

Virginia Modeling, Analysis and Simulation Center,
Old Dominion University
www.vmasc.odu.edu

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

**Health and medical
readiness**

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Regional burn care

Moderator

Kevin Hayden
Director for Planning,
Initiatives & Development,
Department of Health
and Senior Service,
State of New Jersey

Panelists

Chris Ruhren MAS, RN, CCRN
Director of Burn, Critical
Care, Emergency Services,
St. Barnabas Medical
Center, Livingston,
New Jersey

Jim Howson
Director, Burn MCC,
Emergency Management
Corporate Division

Theodore Tulley
Director of Trauma and
Emergency Services,
Westchester County
Health Care Cooperation,
Valhalla, New York

The treatment of burn victims requires a great deal of resources in terms of specialized training and equipment. In a mass-casualty event the existing capacity of dedicated burn centers can rapidly be overwhelmed. By definition, this means that burn victims will have to be triaged and transported to facilities that can handle them. This, in turn, requires extensive coordination throughout the healthcare system – hospitals, transportation agencies, first responders – throughout the region and beyond.

Building on experience gained from 9/11, when almost 1,500 patients were evacuated from the southern tip of Manhattan, New Jersey has been working to develop a coordinated overall surge capability to deal with the mass-casualty issue, as well as a dedicated burn coordination capability. This innovative program is in its third year. This session detailed these efforts and also discussed parallel and complementary efforts being undertaken in New York, as well as issues to be taken into consideration when planning for burn care.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Highlights

- New Jersey has set up a series of Medical Coordination Centers (MCCs). The MCCs are tasked with a variety of responsibilities both before and during an emergency:
 - Prior to an emergency, development of regional healthcare planning, training, exercises and information gathering within municipal, county and state public health, health-care and EMS systems.
 - During an emergency, communicating information on hospital diversion status, healthcare facility bed status, pharmaceutical stockpile availability, medical information, epidemiological information and EMS status.
 - Integrating, coordinating and communicating with public health and healthcare systems both intra- and interstate, based on national priorities.
- MCCs are set up in shared facilities that are also used for training, to minimize costs. In the event of an emergency, the MCC function pre-empts other uses of the facility.
- The MCCs are designed to coordinate within and among existing organizational structures and protocols, rather than “reinvent the wheel.”
- The state is divided into five healthcare regions that reflect population density. There are nine MCCs in total; regions that have more than one MCC have a designated “host” MCC. In addition, there is a single command center.
 - The MCCs provide statewide standardization, but regional specialization – i.e., the specifics of each MCC are tailored to the needs of its region.
- Coordination of healthcare activities extends beyond hospitals and includes EMS, long-term/home healthcare, blood banks, etc.
 - There is a geographical information system (Hippocrates) that helps determine the status of all facilities in the region to help determine where to send patients.
- There are four levels of activation for the MCCs. The level of activation is situation-dependent. Each successive level of activation brings in more staffing. The lowest level, daily operations, has a single facility manager staffing the center. The highest level adds a state Department of Health and Senior Services/MCC coordinator and staffs all MCC functional positions.
- A dedicated Burn MCC is located at St. Barnabas, which is the only burn facility in the state (30 beds).
 - There are only 127 dedicated burn centers in the country, with a total of approximately 1,800 burn beds. In the Northeast, from DC to Maine and everything east of Pittsburgh, there are only 353 dedicated burn beds. The number of centers is dropping due to the cost of operations. The number of beds available in a disaster is always less than the total because of existing patients.
 - A 2005 assessment in New Jersey polled non-burn-center assets to determine the level of capability. A tier matrix system was put in place to identify the level of care that each facility is able to provide. This information was used along with survival rate data from the American Burn Association to develop triage guidelines.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

**Health and medical
readiness**

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- It is not appropriate to send all victims to a burn center due to capacity limitations. Those with either too great or too low a chance of survival should be sent to Tier II, III and IV healthcare facilities, according to the guidelines. Smoke inhalation in addition to burn alters the guidelines.
- A basic mission of the Burn MCC is to coordinate the allocation of these patients and track information regarding them.
- The Burn MCC has developed protocols for triaging and moving burn patients as well as gathering and providing information. The Burn MCC also serves to alert the healthcare system that an incident which will generate a significant number of burn patients has occurred.
- The Burn MCC also provides standardized education for first responders and lower-tier hospitals to create a coordinated, standardized response that is appropriate to a disaster, e.g., EMS normally would send a burn victim straight to the burn center, but in an emergency that patient might have to go to a different facility.
- Burn centers may actually be too much of a specialized resource in a disaster scenario, because EMS will try to send all burn victims to the burn center. In the London bombings, the response was more appropriate because there were only regular local hospitals, so patients were spread appropriately.
- Depending on severity, burn victims can be staged. A given burn victim might survive three or four days in a regular hospital while the surge passes, and be transferred to a burn center at a later date.

- The Burn MCC is implementing videoconferencing to enable it to provide telemedicine, thereby leveraging burn-specific expertise for facilities that lack it. Telemedicine is a focus in New York as well.
- Transportation of burn victims needs to be coordinated and resources leveraged appropriately. If ground transport will suffice, it makes no sense to use a helicopter. Transportation coordination and planning is missing from many surge plans.

Resources

American Burn Association
www.ameriburn.org/

St. Barnabas Burn Center
www.saintbarnabas.com/calendar/cable/burnctr.html

N.J. Dept. of Health and Senior Services
www.nj.gov/health/

Westchester Medical Center
www.wcmc.com/

Somerset MCC press release
www.somersetmedicalcenter.com/body.cfm?id=35&ref=977&action=detail

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

**Health and medical
readiness**

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Multi-jurisdictional preparedness with food safety

Moderator

Bill Krueger
Director, Laboratory
Services Division, Minnesota
Department of Agriculture

Panelists

Mickey Parish
Acting Director of the
Center for Food Systems
Security and Safety,
University of Maryland

Alan Taylor
Director, Office of Food
Protection and Consumer
Health Services, Maryland

A terrorist attack via the introduction of pathogens, chemicals and/or other harmful substances into our food (either crop or livestock) and water supply has emerged as a very credible and significant concern. In the greater Mid-Atlantic region, the \$280 billion food system sustains 46 million residents and is a key component of the national and international food production and distribution infrastructure.

Highlights

- Agriculture and food combine to make up 12.3 percent of our GDP, one in six jobs are somehow related to it and panelists estimate that as much as 20 percent of our economy is involved with agriculture and food.
- With the billions that have gone to Homeland Security, and other agencies such as CDC, to help strengthen our public health infrastructure, very little has gone into the food and agriculture sector.
- One panelist related the results of tabletop scenarios, wherein participants simply took some garden-variety poisons and disseminated them, imagining 10 terrorists contaminating various food sources and grocery stores.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

At the end of a few days, the scenario showed CNN announcing that 28 states had 12,000 cases of Salmonella typhi, 895 deaths by cyanide, and 425 rat-poisoning deaths.

- The panelist asked pointed questions, based on this scenario: Where are you going to buy your food tomorrow? How long does it take us to recover? How do we then create safe distribution channels? How long before we can restore confidence, so that a person doesn't go to the next-door neighbor with a gun and say "I want some of your canned goods because I know you have them, my children have to eat." At what point does our culture break down?
- It's not a new strategy to use food and agriculture as a means of weaponry to try to take out your adversary. It goes back as early as 1600 BC.
- One panelist pointed out that in China rat poisoning seems to be the method of choice of taking out your competitor.
- In America, if toxins were put in a single bulk tank of milk, if you look at the disbursement throughout the country and how milk is transported, the numbers are staggering: over 100,000 deaths could result.
- But how do you protect food and agriculture? You can easily designate a bridge as part of critical infrastructure, and rebuild that bridge if necessary. But we don't have a bridge that we're trying to protect, we're trying to protect a system.

For example, Minnesota gets somewhere around \$30 million to protect its infrastructure; none of that is going into food and agriculture because they can't define the critical assets that they're trying to protect.

- More predictive modeling is needed in order to strategically make the investment set that best protects and defends our food supply.
- According to the University of Maryland, food defense is putting a system in place to prevent, protect, respond and recover from intentional introduction of contaminants into our nation's food supply that are designed specifically to cause negative public health, psychological, and/or economic consequences.
- We have been attacked. In 1984 a cult purposely contaminated salad bars in an attempt to affect the outcome of the local county elections. It took FBI about a year to link the illnesses with that cult, as the food regulatory chain is highly complex.
- Defending the food supply is highly complex. There are multiple regulatory authorities involved, and the food industry itself is greatly concerned.
- Maryland has representatives regularly attend meetings of the Maryland Delaware Agro-Terrorism Working Group, chaired by the FBI.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- The Maryland Department of Agriculture does industry audits and information sharing, distributes the pamphlets that were generated from the USDA and the FDA and the Food Defense and Agricultural Security and engages in collaborative efforts with partner agencies.
- However, until criticality studies are completed and predictive modeling is done, until you can actually identify what critical food infrastructures you need to protect in your locality, the larger dollars are not going to be redirected; so, the states that are getting funded US\$20 million to US\$40 million a year can't redirect it to the food and agriculture until we have those studies done.

Resources

Minnesota Department of Agriculture
www.mda.state.mn.us/

Center for Food Systems Security and Safety
agresearch.umd.edu/CFS3/index.cfm

Office of Food Protection and Consumer Health
Services, Maryland
www.cha.state.md.us/ofpchs/

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Information sharing and intelligence

▶ Fusion center update

▶ Data sharing tools

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

**Information sharing
and intelligence**

Law enforcement

Public safety
communication and
interoperability

Fusion center update

Moderator

Captain Charles Rapp
Baltimore County
Police; Director,
Maryland Coordination
Analysis Center

Panelists

Jack Tomarchio
Principal Deputy
Assistant Secretary,
Office of Intelligence
and Analysis, DHS

Tom Finan
Director, Intelligence
Subcommittee,
House Committee on
Homeland Security

Some 58 fusion centers have been established across the country and are now beginning to produce high-quality intelligence products, though the centers, their structure and their operational models have not reached full maturity as yet. This session covered the current state of these centers, the challenges facing them, anticipated directions, the effect of recent federal initiatives and some recommendations on how to improve their effectiveness.

Highlights

- Federal initiatives have emphasized the important role of fusion centers as a key part of the homeland security and all hazards mosaic.
 - The 9/11 Recommendations Act, signed into law in October 2006, includes guidelines for federal support of state fusion centers in the form of DHS and FBI personnel presence, looking to the local fusion centers to define what is needed in terms of intelligence products in each state or region, rather than mandating it from Washington, establishing the counterterrorism as well as law enforcement capabilities of each fusion center.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

–The National Strategy for Information Sharing, an October 2007 Bush Administration policy document, lays out White House support for the central/leading role of fusion centers as the point of information sharing between the federal government and state, local and tribal partners; explicit statements regarding federal funding, technical and training support; and the definition of appropriate roles for the fusion center.

- The fusion center concept is still relatively new and has yet to reach full maturity. There is no “one-size-fits-all” model for the structure and operation of a fusion center, because different regions have different requirements. Some states have no fusion center, nor is it likely that they need one.
 - A possible future direction is the idea of regional fusion centers where they make sense, instead of state fusion centers.
- There is a clear understanding at the federal level that local leaders know best what kinds of assistance is needed and relevant, but there is substantial value in having federal (DHS and FBI) personnel on-site at the fusion center. By the end of FY 2008 there should be 35 DHS officers deployed.
 - Federal personnel should be integral team members, not mere liaison officers. This helps to forge the trusted relationships needed for effective information sharing.
 - DHS officers have different roles at different fusion centers.
 - The level of presence needs to be tempered by actual requirements.

- Interoperability has come a long way in the past few years, with fusion centers sharing information with one another and with the federal government to a greater extent. This improves the quality of intelligence generated and can help analysts spot patterns that may not be apparent at the local level.
- The information and intelligence products generated by the fusion center need to be relevant to local needs first and foremost.
 - The intelligence community sees great value in merging intelligence developed locally with national intelligence from DHS, FBI and NCTC in order to develop better situational awareness.
- Sustainability of the fusion center concept is an issue, particularly with regard to funding and continuity.
 - Fusion centers in the same region can group together to share resources and apply for funding. Interoperability and collaboration helps make resource use more efficient.
 - Continuity needs to be planned for, in terms of staffing turnover.
 - Funding is more readily obtained if the fusion center can establish the value of its products and prove that the money is well spent.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Training for intelligence analysts is available, but, at present, requires taking personnel off the job and having them travel. This is not viable for most fusion centers, so there is a need to develop training programs that can be conducted on-site.
 - There is a need to develop a “common language” and understanding between law enforcement and intelligence personnel to facilitate information sharing.
 - The use of classified material in training programs is an issue.
- Privacy laws and civil rights are a concern for fusion centers and information sharing in general.

Resources

GAO Homeland Security report, October 2007:
“Federal Efforts Are Helping to Alleviate Some Challenges
Encountered by State and Local Information Fusion Centers”
www.gao.gov/new.items/d0835.pdf

National Strategy for Information Sharing
www.whitehouse.gov/nsc/infosharing/index.html

9/11 Recommendations Act
www.govtrack.us/congress/bill.xpd?bill=h110-1

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

**Information sharing
and intelligence**

Law enforcement

Public safety
communication and
interoperability

Data sharing tools

Moderator

Warren Campbell
Assistant Director,
Technical, Maryland
Emergency Management
Agency (MEMA)

Panelists

Michael Pack
Lab Manager, RITIS Project
Manager, University of
Maryland Center for
Advanced Transportation
Technology Lab

Thomas Henderson
Executive Director,
CapWIN

Matt Felton
Director, Towson University,
Center for Geographic
Information Sciences

Mosi Kitwana
Director of Results
Networks, International
City/County Management
Association

Over the past several years many very successful initiatives have been undertaken in the area of sharing information among government agencies and first responders. Some of these initiatives have distinct and unique purposes, while others have overlapping capabilities.

This session detailed four such systems currently in use in the National Capital Region (NCR):

- WebEOC, the Maryland Emergency Management Agency's Web-based incident management system that integrates and funnels data from many sources.
- Emergency Management Mapping Application (EMMA), from Towson University, which integrates and funnels a wide variety of geographical data.
- Regional Integrated Transportation Information System (RITIS), from the University of Maryland, which integrates and funnels transportation data.
- Capital Wireless Information Net (CapWIN), a wireless system that is analogous to WebEOC.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

In addition, a fifth initiative has been independently developed and is being rolled out in other parts of the country:

- National Emergency Management network, which is similar to WebEOC and CapWIN. However, it also includes additional planning components.

A common thread running throughout each panelist's presentation was the idea of continuous development and refinement of these systems. A system is implemented, then enhanced and adjusted based on lessons learned on an ongoing basis. Therefore, the state of these systems was not preplanned – they have evolved over time, and continue to do so. This also applies to usage: as users see what can be done, they think of new ways to use the technology.

Highlights

WebEOC

- WebEOC is a Web-based incident management tool. MEMA issued an RFP for the system and got proposals ranging from US\$46,000 to US\$2 million. The least expensive proposal was chosen, but not because of cost. Rather, it was because the system met key criteria:
 - It was simple and intuitive, requiring a minimum of training and easy to pick up on weeks or months later.
 - It was flexible and did not require any change of policy or procedure to fit the solution.

- This eased acceptance and, in fact, resulted in changes to operations. It was demonstrated that things could be done better; the software facilitated change, but did not require it.
- The system's flexibility and simplicity has allowed MEMA to build custom capabilities into the software as the system evolves, with no need for technical expertise.

- WebEOC is now used by every local jurisdiction in Maryland, as well as all law enforcement agencies (down to the level of campus police at state-sponsored schools), all state agencies and departments, as well as the District of Columbia and Virginia.
 - Universal acceptance means a common platform and common picture of the current situation, 24x7, in real time, available throughout the state and beyond.

- WebEOC is built on a network of separate IT systems owned by different agencies. This spreads operating expenses and enhances resiliency.
- WebEOC is in essence an information aggregator. Input comes from a wide variety of sources ranging from individual users (e.g., a state trooper responding to an accident) to the output of complete systems (e.g., EMMA, RITIS).
 - Any kind of data can be integrated and presented, from text to video to data streams.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Common access to information across jurisdictional and agency boundaries has resulted in a need to adopt standard definitions and terminology (e.g., a “tanker” for fire fighting might mean a water-drop aircraft in California, but a water-filled truck in another state). FEMA has defined 140 distinct types of resources to address this issue, and Maryland has added an additional 70.
- Future goals include greater integration with other systems, such as the federal Homeland Security Information Network. This would prevent duplication of effort, by allowing Maryland to push incident data to HSIN when necessary without having to re-key it.

EMMA

- An initiative separate from WebEOC, EMMA is the result of an early recognition by the state that there was a rich resource of geospatial data available, and that it could be leveraged to enhance the capabilities of WebEOC. EMMA serves Maryland as well as surrounding states.
- The common thread among all incidents, no matter what their size or how dynamic they may be, is geography. Data that might not otherwise fit together in an understandable manner are easily related when viewed on a map.

- EMMA provides layers of diverse data drawn from many sources. For example, a hospital might be depicted on a map. Information about that hospital (e.g., is it full?) can be attached to that point, as well as current weather at that location, or any other conceivable piece of data that is linked to the system. Information about anything on the map can be displayed by clicking on the location.
 - The data layers can be filtered according to need, to reduce clutter.
- All of this geospatial data is fed to WebEOC.
- Based on input from local emergency managers, EMMA was built to provide five key capabilities:
 - Location of incidents and resources.
 - Ability to generate a quick location report (what’s happening there?).
 - Ability to easily customize the map view to suit needs.
 - Ability to make queries and run analyses (e.g., display all schools within five miles of the incident, or display a chemical plume projection based on current winds).
 - Ability to facilitate coordination of resources in real time.
- Some EMMA representations leverage real-time data feeds (e.g., USGS stream gauges, NOAA weather reports).

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Simple, seamless integration with other resources such as WebEOC is critical. This is accomplished in part by pre-defining views as needed.
 - For example, in the case of a power outage, a button can be quickly and easily created for WebEOC users that says, in effect, “Show me the areas that have no power at this time.” This keeps users from having to make intensive use of tools for commonly needed information.
 - Another example is to vary the presentation of geospatial data according to user preference. Some users prefer lists, others maps.
 - Integration is further enhanced by the ability to export data from WebEOC for reporting purposes.

- Goals are to simplify the map tools, address the issue of keeping data fresh, address the issue of quick access to secure data, improve redundancy/continuity, work on standardizing visual representations, develop more analytic capabilities and find ways to share investment and costs.

RITIS

- RITIS ties together traffic data from traffic management centers throughout the state in a manner similar to EMMA's integration of geospatial data. This includes video feeds, data from traffic detectors, sign messages, construction information, police information, etc. RITIS can also integrate other types of data such as weather conditions.
- Like the other systems, RITIS is an information aggregator that pushes data out to users. A key goal of the system is to make it transparent, rather than impose another interface on the user.

- RITIS is designed to feed existing systems such as WebEOC, but it also can feed data directly using a Web interface.
- RITIS also archives data for reporting and analysis.
- Lessons learned include the difficulty of negotiating to obtain access to data, technical interoperability issues, concern over data quality and coordination of integration work.
- Goals are to develop future forecasts, increase video coverage and develop interfaces for mobile users.

CapWIN

- CapWIN is a Web services-based system that essentially parallels WebEOC, but is targeted at wireless users in the NCR (though it can also be accessed through hard-wired lines or the Web). It also provides additional capabilities.
- The system provides four primary service components:
 - Database query.
 - Incident management system (similar to WebEOC).
 - Messaging.
 - Directory of users, with skills and qualifications noted.
- Most use the full suite, but not all users require all services, so the system is designed to be modular.
- CapWIN has dedicated client software. The primary reason for this is robustness; should there be a signal interruption, a standard Web browser would lose all data. The CapWIN client buffers data so it can continue to operate until the signal is restored.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

–The software was designed to be used outdoors in sunlight, as well as at night. It has an easy-to-use touch screen, and is designed to take up as little space on a display screen as possible.

–The system can also be accessed by other means, e.g., through dedicated hard-coded access by existing systems.

- Goals include tighter integration with other systems and the addressing of redundant capabilities that are also provided by other systems such as WebEOC.

NEM network

- The National Emergency Management (NEM) network parallels the WebEOC and CapWIN concepts, but adds interoperability and governance aspects as well. For example, it ties together local and regional emergency managers to form predefined, prequalified response teams that can be deployed very quickly.
- The NEM network's technology components have been developed to support these teams.
- NEM also tracks costs information as well as incident data.

Resources

MEMA
www.mema.state.md.us

WebEOC
www.esi911.com

CapWIN
www.capwin.org

RITIS
www.ritis.org

ICMA
icma.org

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Law enforcement

- ▶ Law enforcement perspectives on human trafficking
- ▶ Law data sharing standards and suspicious activity reporting

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Law enforcement perspectives on human trafficking

Moderator

Mel Blizzard
Director, Metropolitan
Washington, DC Fusion
Center, Commander,
JTTF and Synchronized
Operations Command

Panelist

Carla Proudfoot
Maryland Center for
Missing Children

Panelist spoke about current methods in place to
find missing and/or abducted children.

Highlights

- 74% of children who are abducted by a non-family member are dead within three hours. Most often children are abducted for sexual purposes and usually the perpetrator wants to commit the crime and then get rid of the child as fast as possible. Most of the time they're abducted within a 50-mile radius of the home, or closer, and most often their bodies are recovered within a 50-mile radius of their home.
- In 1982 the Missing Children's Act was passed. That enabled missing children's information to be entered into the National Crime Information Center's (NCIC) computer system. Prior to that there was not a national system where law enforcement could access that information
- Every state has a missing children clearinghouse.
- Clearinghouses are connected through a secure network and exchange information daily. This is strictly an information sharing structure. If a child, for instance, is known to be on a bus in Maryland and headed for California, the clearinghouse can create a poster within minutes of having a photograph, notify the California clearinghouse and ask them to distribute that poster to patrol units in that particular area. Somebody can be waiting at the bus station when the kid gets off the bus.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- All but one of the clearinghouses are housed within a law enforcement agency.
- Each clearinghouse is responsible for receipt, collection and distribution of general information and annual statistics regarding missing children, as well as coordination of law enforcement agencies and other interested persons or groups within and outside the state regarding information on missing children.
- All information also appears on the National Center for Missing and Exploited Children's Web site which gets two million hits a day.
- When a law enforcement agency first receives a report of a missing child it must determine if this is the first time the child is missing, if the child suffers from mental/physical handicap or illness, if the child has been reported to be the victim of any sort of abuse, if the child is under 14 years of age and if the event is of a suspicious or dangerous nature.
- Once these factors have been determined, law enforcement must enter all necessary information into the NCIC, institute appropriate intensive search procedures and notify the National Center for Missing and Exploited Children.
- There is no nationwide AMBER Alert system. An AMBER Alert can be issued if:
 - The missing child is under 18.
 - Law enforcement verifies that a child has been abducted.
 - Law enforcement believes that the circumstances surrounding the abduction indicate the child is in serious danger of bodily harm or death.

- There must be enough descriptive information about the child, suspect or suspect's vehicle to make an immediate broadcast alert beneficial.
- The abductor and/or child are likely in the broadcast area.
- All data elements have been entered into the NCIC system.

- Only a law enforcement agency is eligible to request AMBER Alert activation. If activated, law enforcement works together with radio and television stations to immediately interrupt programming and broadcast information about child abduction by using the Emergency Alert System (EAS). This system is typically used for weather and other civil emergencies. The goal is to alert the public about the missing child as quickly as possible, which may increase the chances of the safe recovery of the child.
- The National Center for Missing and Exploited Children is capturing information on all of the attempted child abductions occurring across the United States. They're beginning to develop a database to attempt to match up an individual by his/her description or the vehicle that he/she is using in attempted abductions from state to state.

Resources

National Center for Missing and Exploited Children
www.missingkids.com

Web-based Amber Alerts
www.codeamber.org/

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Law data sharing standards and suspicious activity reporting

Moderator

Harvey Eisenberg
Assistant U.S. Attorney,
Chief of National Security
and Anti-Terrorism Advisory
Council Coordinator,
District of Maryland

Panelists

Captain Charles Rapp
Baltimore County Police
Department Director,
Maryland Coordination
Analysis Center

Aaron Gorrel
President and CEO,
Waterhole Software

David J. Roberts
Principal, Global Justice
Consulting; Editor-in-Chief,
Public Safety IT magazine

This panel included an executive overview and update on the National Information Exchange Model (NIEM). The Suspicious Activity Report (SAR) is the first national priority exchange that was identified by the program manager for the Information Sharing Environment. The SAR project uses NIEM for a common vocabulary that will permit the exchanges regardless of the type of system being used by a police department or fusion center. The SAR project goes beyond law enforcement to military force protection and critical infrastructure.

Highlights

- NIEM, the National Information Exchange Model, is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprisewide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.
- There are a variety of situations where organizations need to share and exchange information in real time. In some cases, it becomes not only a national but an international security priority. Information must be shared across agencies, across disciplines between agencies and at all levels of government, and there are host of reasons for doing it.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Right after 9/11 information sharing focused on terrorism. We need to be able to share information for terrorism, natural disasters, to respond to organized criminal activities, but we also need, first and foremost, to do it for the day-to-day operations of justice and public safety and emergency management agencies nationwide.
- NIEM is really a data standard with agreed-upon terms, definitions and format.
- There is common data that is useful to all law enforcement agencies. The panelists advocate identifying areas of data. Law enforcement should be able to reuse components and identify source documents that are common – build them a single time and reuse multiple times to accelerate data access.
- This should improve public safety by giving people information much more quickly. For example: when law enforcement pushes information to the prosecutor to initiate a charging document in Maryland, it's the same information used in California, and in every jurisdiction in Colorado. So law enforcement shouldn't have to build that document 5,000 times across the country. NIEM would build it a single time and then reuse it.
- The need for a SAR: People identified as Middle Eastern were associated with suspicious activity on a number of the ferries in the Puget Sound area. They were taking photographs of the ferries. Passengers and crewmembers recognized this activity and over a period of time at least six ferries underwent this potential surveillance by these suspected terrorists.

At the end of July 2007 Washington State police issued a high priority alert. The fact that it took almost 2.5 months for an alert to be issued was a problem in the fundamental system of paper-based exchanges.

- To date, 220 elements have been identified as key elements for inclusion in an SAR. Such as: what activity was observed, what were the facts surrounding the observation by the witness, what potential critical infrastructure are targeted, what is the location of that, who owns it and information about the witness. Further, do you have information about subjects, such as names, vehicles, dates of birth and plate numbers?
- The National Capital Region's Information Exchange Packet Documentation Clearinghouse will be releasing technical and functional specifications for the Suspicious Activity Report, as well as developing a program for starting to work with local, state and regional law enforcement agencies on how to implement NIEM and SAR.

Resources

National Information Exchange Model
www.niem.gov/

Suspicious Activity Report
www.occ.treas.gov/index.htm

National IEPD Clearinghouse
www.ncrnet.us/iepdclearinghouse

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Public safety communication and interoperability

- ▶ Common language/Plain talk initiatives
- ▶ SAFECOM interoperability guidelines and practitioner methods of implementation
- ▶ Living interoperability planning

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Common language/Plain talk initiatives

Moderator

Chris Essid
Interoperability Coordinator,
Commonwealth of Virginia

Panelists

Chief Charles Werner
City of Charlottesville,
Virginia Fire Department

Mike Roskind
Deputy Director, DHS,
Office of Emergency
Communications

The Commonwealth of Virginia, to comply with the National Incident Management System (NIMS) requirements with regard to common language protocol, established an initiative action team of practitioners to help work toward a statewide common language protocol in December 2005.

Specifically, the NIMS Communication and Information Management Recommended Activity is to use plain language – apply standardized and consistent terminology, including the establishment of plain language communications standards – across your organization and when you are communicating with other private sector partners and local emergency management organizations. NIMS states that achieving effective communications, information management and information- and intelligence-sharing are critical aspects of domestic incident management, and when operating in a multi-discipline and multi-jurisdictional incident, common language among all responders limits confusion and miscommunications.

The Common Language Protocol is designed to enable public safety officers to use plain English for day-to-day radio communications and a limited number of statewide coded transmissions to ensure responder safety.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Highlights

- While "10 codes" were intended to be a concise and standardized system, the proliferation of different meanings has rendered it useless for situations where people from different agencies and jurisdictions need to communicate.
- 10 codes are different all over the nation. The panelists cited examples where in one locality a given 10 code means an officer is using the restroom, in the neighboring locality it means officer down, and in the next locality it means a burglary in progress. This can lead to conflicting reports and garbled communications in an era where we are moving towards increasing mutual aid situations across local and regional boundaries.
- Virginia was the first state in the nation to move towards implementing a Common Language Protocol.
- The state formed an initiative action team, and followed a practitioner-driven process, allowing the personnel that respond to the fires, and carry out the law enforcement and EMS responsibilities to move the state towards accomplishing common language protocols.
- The first problem the team found was that NIMS calls for responders to use common language only in mutual aid situations, when responders from different departments or

jurisdictions may be coordinating efforts. The team determined that responders would need to use common language on a daily basis, as they believed responders would revert to their basic training in crisis situations.

- However, some situations must be seen as exceptions, given that common language used aloud may put responders in danger. Specifically, the panelist used an example of a police officer pulling over a wanted terrorist, and the dispatcher broadcasting that intelligence aloud, within hearing of the suspect.
- The four scenarios that need some kind of a coded language, are:
 - Responder in immediate danger.
 - Responder needs back up or assistance.
 - Responder recommends taking a subject into custody.
 - Responder or dispatcher needs to convey sensitive or confidential information.
- The Virginia team held 14 meetings and 23 conference calls before reporting the recommendation to the State Interoperability Executive Committee. In October 2006, Virginia announced the Common Language Protocol for day-to-day operations and major emergency situations, and became the first state in the nation to do so at a state-wide level.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- Beyond common language protocols, panelists also pointed out that specific radio frequencies/channels needed to be named and recognized for use in mutual aid situations.
- The National Public Safety Telecommunications Council (NPSTC), is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leaderships. Panelist urged attendees to consider participating with NPSTC in some of the working groups and become involved with other mutual aid and interoperability issues such as channel naming.

Resources

National Incident Management System
www.fema.gov/emergency/nims/index.shtm

National Public Safety Telecommunications Council
www.npstc.org/index.jsp

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

SAFECOM interoperability guidelines and practitioner methods of implementation

Moderator

Marilyn Praisner
NaCo/Chair of Executive
Committee, SAFECOM

Panelists

Chris Essid
Interoperability Coordinator,
Commonwealth of Virginia

SAFECOM is a communications program of the Department of Homeland Security, tasked with providing research, development, testing and evaluation, guidance, tools and templates on interoperable communications-related issues to local, tribal, state and federal emergency response agencies. The SAFECOM Executive Committee (EC) works with the DHS Office of Emergency Communications (OEC) and Office of Interoperability and Compatibility (OIC).

An important role for SAFECOM has been to drive the creation of workable interoperability plans at the state level. The first of these is Virginia's Statewide Communications Interoperability Plan (SCIP), which has been used as a template by other states, that were required to submit their own interoperability plans in December 2007 to qualify for a one-time federal funding opportunity.

This session covered general observations about the operation of SAFECOM as a whole and the experience of Virginia in implementing SCIP, as well as examples of progress.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- SAFECOM is working to broaden local government understanding and increase opportunities for participation, communication and collaboration throughout the government and first responder community.
 - SAFECOM gives elected officials the tools they need to ask important questions regarding interoperability.
 - Misperception can be an issue. It is not always recognized that those working for interoperability are actually representing the entire first responder community as opposed to just one part of it (e.g., fire).
 - Individual problems may seem unique, but often have common characteristics that can be addressed through collaboration.
 - There is no “cookie cutter” process that can be applied across the board.
 - Listening to other stakeholders, understanding their challenges and finding common ground is essential for success.
 - Tangible, reportable progress is important to show that the process works.
- While the “usual suspects” issues surrounding interoperability (such as funding, training and exercises and technical standards) are of ongoing concern for first responders, governance and structure have shown themselves to be of equal importance.
 - Sustainability, not only in terms of funding, but also in terms of carryover across administrations, is a critical consideration.
 - In 2007, it is estimated that Virginia spent 12,000 man-hours solely on implementation of interoperability plans. The Commonwealth Interoperability Coordinator's Office has a full-time staff of 11.
- It is important that elected officials and administrators connected to the interoperability issue be actively engaged with those who are directly affected by it (i.e., first responders) as well as their own counterparts from neighboring states and jurisdictions.
- Data communications has assumed new importance in interoperability planning as awareness of its importance grows. SAFECOM is working on including data communications in all of its deliverables.
 - Once police are exposed to the kind of data they can obtain, their demand for more information skyrockets.
 - While there are some technical challenges that need to be worked out, such as bandwidth and protocol issues, these are in some cases minor compared to governance issues such as compliance with privacy legislation and protection of sensitive information (need to know).
 - Some states tackle data interoperability first (Maryland), while others target voice interoperability first (Virginia). These states can learn from one another to accelerate their own efforts going forward.
- SAFECOM advocates a bottom-up, practitioner-driven approach that begins with first responders.
 - To bypass DHS bureaucracy, in 2007 SAFECOM's Emergency Response Council (ERC, made up of first responders and charged with providing guidance and input to the SAFECOM EC) created action teams to review interoperability principles and provide assurance that local communities will endorse plans that include those principles. ERC practitioners serve as peer reviewers of SAFECOM's work.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- The bottom-up approach helps “sell” an interoperability initiative because those who are directly affected by it are the same people who helped create it. By contrast, some DHS edicts come down from the federal government and are not as well received.
- Virginia uses a similar approach that includes direct participation by practitioners. They provide guidance and advice to the governor’s office and have been able to identify real-world issues that only practitioners would uncover.
 - The large number of practitioner participants engaged in the development of Virginia’s SCIP process resulted in findings that otherwise would have been missed.
 - In Virginia, the commonwealth has been divided into seven homeland security regions, each represented by a regional preparedness advisory committee (RPAC) consisting of all stakeholders.
 - Virginia has created initiative action teams to tackle specific issues, such as the transition from “10 codes” to common language.
 - 78 percent of Virginia has made the transition, but there has been resistance to shifting away from 10 codes.
 - The shift is necessary because neighboring jurisdictions may have vastly different 10 codes in use, for example the same code might mean “restroom break” in one locale and “armed robbery” in a neighboring locale.
 - There is a loophole in the NIMS common language requirement, which requires common language only in mutual aid situations. Virginia practitioners recognized that it needs to be used at all times, because in a real emergency, people fall back on familiar habits and the tools they use every day.

- There is still a need for coded language in some situations where plain language might put an officer at risk, such as the need to transmit sensitive information. These codes should be made consistent.
 - In Virginia’s radio cache initiative, practitioners were called on to define the requirements for what goes into the three caches around the state, including radios that can cover all frequencies and common equipment and cross-training for all cached resources.

Resources

SAFECOM
www.safecomprogram.gov

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Living interoperability planning

Moderator

Rocky Lopes
Project Manager for
Homeland Security, NACo

Panelists

Chris Essid
Interoperability Coordinator,
Commonwealth of Virginia

Matt Foosaner
MA, CBCP, CHS-III, Sprint,
Director, Emergency
Response Team

Dr. Kenneth Budka
Director, Public Safety
Wireless Research,
Bell Technologies

This session covered some of the practicalities of interoperability planning, including the impact of the Public Safety Interoperable Communications (PSIC) grant program proposals (due December 2007) on planning and the future implications surrounding the January 2008 auction of 700 MHz spectrum by the FCC.

Much of the session described Virginia's Statewide Communications Interoperability Planning (SCIP) methodology, begun in 2004 and resulting in one of the first statewide interoperability plans in the nation. The SCIP methodology has been adopted by many states as a model for developing plans to submit for PSIC grant funding.

PSIC is a grant program administered by the Department of Commerce National Telecommunications & Information Administration (NTIA). The program provides one-time grants totaling US\$1 billion to assist public safety agencies in the acquisition of, deployment of or training for the use of interoperable communications systems that can utilize a portion of the 700 MHz band (formerly used by analog broadcast television) which has been reallocated for use by those agencies.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

Highlights

Virginia interoperability planning, governance, and the PSIC grant

- SCIP was developed by Virginia with the assistance of SAFECOM. It uses a bottom-up process that is driven by first responders and others who actually use communications on a daily basis (local practitioners). This is a particular strength of the methodology, because the projects that are undertaken are those deemed of greatest importance by the people who use them.
- The first iteration of Virginia's interoperability plan included four overarching goals as defined by local practitioner consensus:
 - Establish communications interoperability as a high priority.
 - Establish the statewide use of a common language and coordinated communication protocols for emergency response.
 - Maximize interoperability capabilities by using existing communications systems, equipment and planning for future technology purchases.
 - Enhance the knowledge and proper use of existing and future communications equipment, systems and resources.
- A critical aspect of interoperability planning as it applies to the PSIC grant process is that all proposed projects must be clearly linked to the interoperability plan and serve it in some way. This level of detail was not needed before PSIC.
 - Not all projects may qualify for PSIC, but there are other funding sources.
 - PSIC money may not become available until late spring or summer, 2008.
 - Since it is a one-time grant, PSIC is intended to fill capability gaps, not fund ongoing initiatives or operations.
- A basic function of interoperability planning is to identify statewide initiatives that will ultimately contribute to seamless interoperability, vet them, coordinate them and find funding. These initiatives take time and cannot all be handled at once; in addition, some are predicated on the completion of others.
- Interoperability governance is a critical of the day-to-day ("living") planning process. This requires a governance structure.
 - In Virginia, needs on the ground are identified by Initiative Action teams, made up of local practitioners. This is in keeping with the "bottom up" approach of the SCIP methodology. It is important to involve local practitioners from all over the commonwealth because the needs of one region may not match those of another part of the commonwealth.

Opening plenary session:
Homeland security
directors' roundtable

Border, transportation,
urban and
campus security

Critical infrastructure
protection

Emergency management

Grants and procurement

Health and medical
readiness

Information sharing
and intelligence

Law enforcement

Public safety
communication and
interoperability

- These teams make recommendations for projects, which are passed to an advisory group that issues guidance and recommendations to an executive committee. This committee is comprised of both state and local/regional organizations, and represents broad-based collaboration. The executive committee ultimately makes recommendations. In addition, there is a coordinating office to administer the entire process.
- Regular meetings are held around the state to keep the process moving and to keep everyone informed.

The implications of interoperability, changing needs and new spectrum

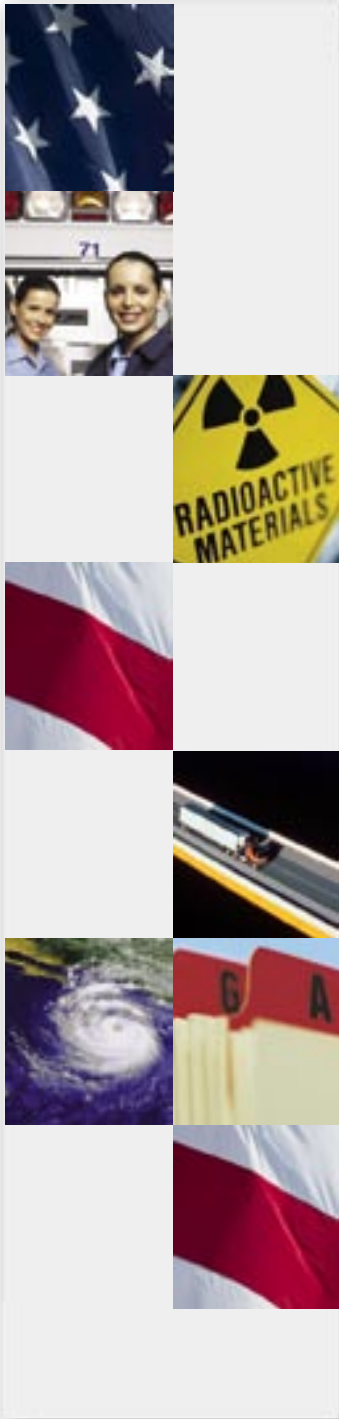
- Increasingly, there is a move away from agency-owned, proprietary systems and towards hybrid systems that are in part owned by private partners. An example is the Sprint/Nextel self-contained, deployable cache of communications equipment that is available to Virginia for use where and when needed.
 - This means that public agencies must be prepared to work closely with private companies in an emergency.
 - Privately owned technology may get updated faster than agency-owned systems, so it has the potential to be more up-to-date.
 - Data communications is becoming increasingly important. Private sector partners can act as advisors regarding future trends and available technologies.

- There is a proposal to create a nationwide shared public/private network using newly reallocated 700 MHz spectrum by 2009.
 - This is a fundamental shift away from earlier thinking, which allocated spectrum solely for public safety.
 - The network will serve private users, but they will be pre-empted by public safety agencies in time of emergency.
 - The revenues generated by private use will help operate and further develop the network, making it self-sustaining.
 - Governance is critical to making the project a reality and has yet to be worked out.

Resources

Virginia Governor's Office of Interoperable Communication
www.interoperability.virginia.gov

PSIC grant information
www.ntia.doc.gov/psic/



Resources

All Hazards Consortium
www.ahcusa.org

Contacts

John Contestabile
All Hazards Forum
Program Chair
jcontestabile@mdot.state.md.us

Tom Moran
Industry/Government
Liaison
tom.moran@ahcusa.org

Other HSPD-8 issues
hspd8@dhs.gov

UTL and CTL
utl@dhs.gov

Presentations

Available presentations for sessions can be found on the All Hazards Consortium Web site: www.ahcusa.org

Web links

*Opening plenary session:
Homeland security
directors' roundtable*

Delaware
dshs.delaware.gov

District of Columbia
hsema.dc.gov/dcema/site/default.asp

Maryland
www.gov.state.md.us/homelandsecurity.html

Pennsylvania
www.homelandsecurity.state.pa.us

Virginia
www.commonwealthpreparedness.virginia.gov

West Virginia
www.wvdhsem.gov

*Border, transportation,
urban and campus security*

James Madison University
public safety
www.jmu.edu/pubsafety

UASI Portal
secure.cityofno.com/Portals/UASI/portal.aspx

Transportation Security Administration (TSA)
www.tsa.gov

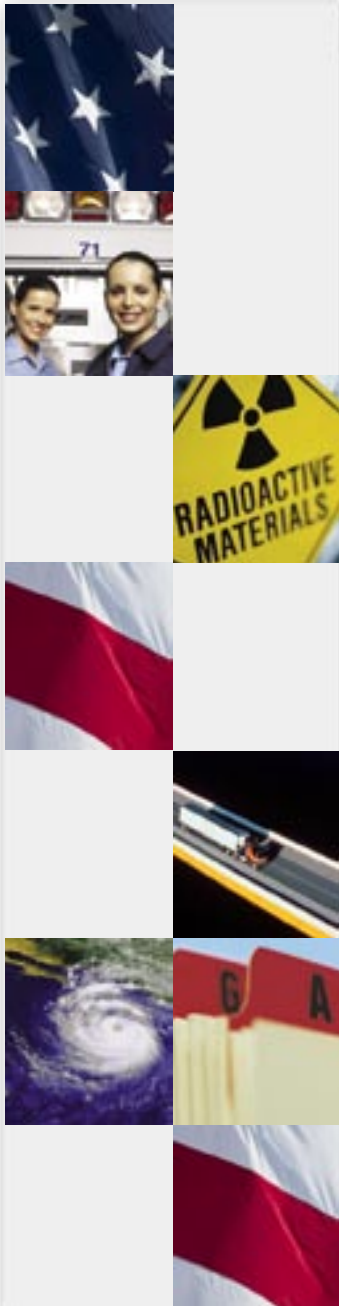
Homeland Security Presidential Directive 12
www.osec.doc.gov/osal/HSPD12/HSPD-12Information.htm

Houston TranStar
www.houstontranstar.org/about_transtar/

Federal Highway information
www.fhwa.dot.gov/index.html

Critical infrastructure protection

ACAMS information
www.dhs.gov/xinfoshare/programs/gc_1190729724456.shtm



Protected Critical Infrastructure Information program
www.dhs.gov/xinfoshare/programs/editorial_0404.shtm

InfraGard home page (overall program)
www.infragard.net/

InfraGard Members' Alliance (member side)
infragardmembers.org/

National Infrastructure Protection
www.dhs.gov/xprevprot/programs/editorial_0827.shtm

Request for fusion center white paper
www.rsvpbook.com/event.php?408404

Homeland Security Presidential Directive 7
www.fas.org/irp/offdocs/nspd/hspd-7.html

Constellation ACAMS
www.dhs.gov/xinfoshare/programs/gc_1190729724456.shtm

Virginia Department of Emergency Management
www.vdem.state.va.us/

EPA Hazardous Site Cleanup Division
www.epa.gov/reg3hwmd/

Chemical Facility Anti-Terrorism Standards
www.dhs.gov/xprevprot/laws/gc_1166796969417.shtm

AHC October meeting agenda
www.ahcusa.org/documents/CIP%20Workshop%20Agenda.pdf

Emergency management

National Incident Management System
www.fema.gov/emergency/nims/index.shtm

FEMA
www.fema.gov/

National Integration Center (NIC) Incident Management Systems Integration Division
www.fema.gov/emergency/nims/

NIMS compliance and technical assistance
www.fema.gov/emergency/nims/nims_compliance.shtm

Eleven NFPA Standards for Emergency Responders
www.nimsonline.com/

Jacksonville, FL EOC NIMS
www.floridadisaster.org/CIEM/

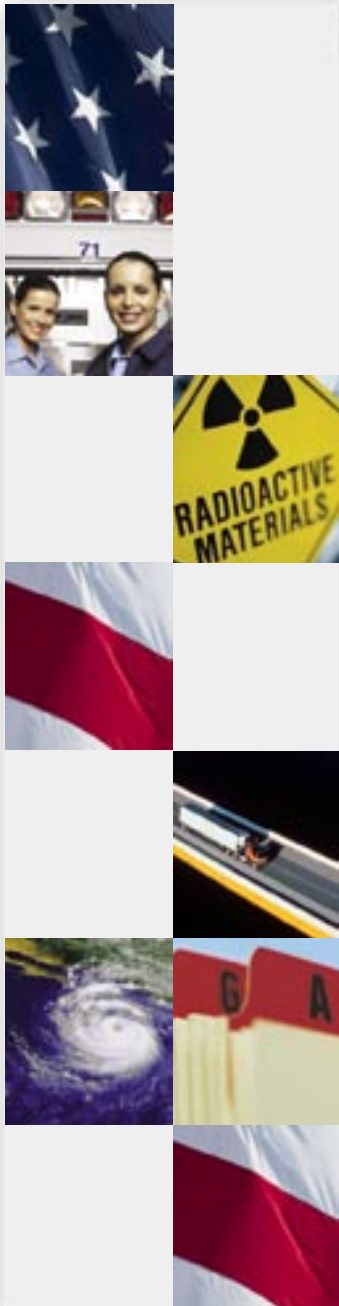
Virginia Child Protection newsletter focusing on gang prevention
psychweb.cisat.jmu.edu/graysojh

The National Traffic Incident Management Coalition
timcoalition.org

National Unified Goal
www.transportation.org/sites/ntimc/docs/NUG%20Unified%20Goal-Nov07.pdf

Forterra Systems
www.forterrainc.com

National Response Framework
www.fema.gov/emergency/nrf/



Department of Homeland Security
www.dhs.gov/index.shtm

Beck Disaster Recovery
www.beckdr.com/

The Infrastructure Security Partnership
www.tisp.org

Washington Metropolitan Area Transit Authority
www.ncrnet.us/iepdclearinghouse

District of Columbia Homeland Security Emergency Management Agency
dcema.dc.gov/dcema/site/default.asp

Montgomery County Homeland Security
www.montgomerycountymd.gov/mcgtmpl.asp?url=/content/homelandsecurity/index.asp

Grants and procurement

Grant guidance from DHS
www.ojp.usdoj.gov/odp/grants_programs.htm

Grant guidance from FEMA
www.fema.gov/government/grant/index.shtm

Fact Sheet: Fiscal Year 2008 Preparedness Grants
www.dhs.gov/xnews/releases/pr_1201882312614.shtm

Office of Grant Operations, U.S. Department of Homeland Security
www.ojp.usdoj.gov/odp/grants_programs.htm

District of Columbia Homeland Security and Emergency Management Agency
dcema.dc.gov/dcema/site/default.asp

Health and medical readiness

Delaware Pandemic Influenza Plan
www.dhss.delaware.gov/dph/files/depanfluplan.pdf

Virginia Modeling, Analysis and Simulation Center, Old Dominion University
www.vmasc.odu.edu/

American Burn Association
www.ameriburn.org/

St. Barnabas Burn Center
www.saintbarnabas.com/calendar/cable/burnctr.html

N.J. Dept. of Health and Senior Services
www.nj.gov/health/

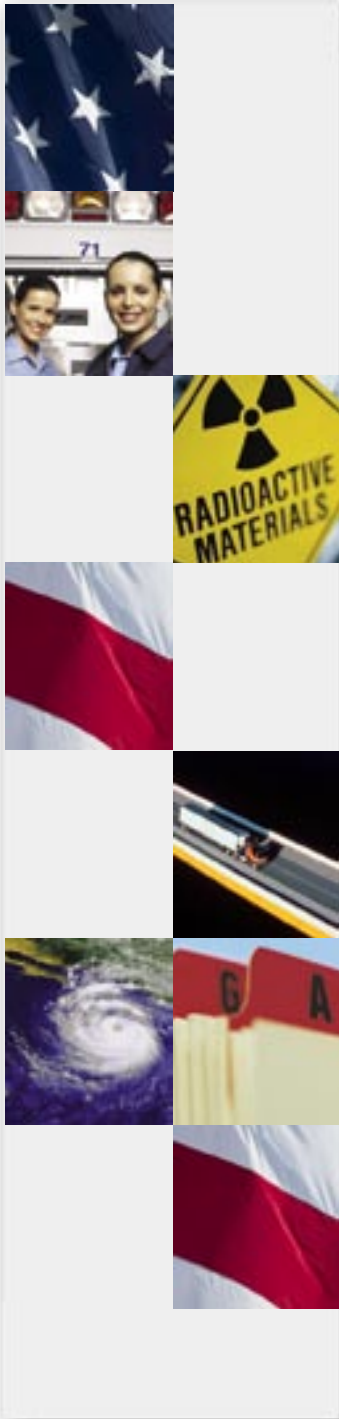
Westchester Medical Center
www.wcmc.com/

Somerset MCC press release
www.somersetmedicalcenter.com/body.cfm?id=35&ref=977&action=detail

Minnesota Department of Agriculture
www.mda.state.mn.us/

Center for Food Systems Security and Safety
agresearch.umd.edu/CFS3/index.cfm

Office of Food Protection and Consumer Health Services, Maryland
www.cha.state.md.us/ofpchs/



Information sharing and intelligence

GAO Homeland Security report, October 2007: "Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers"
www.gao.gov/new.items/d0835.pdf

National Strategy for Information Sharing
www.whitehouse.gov/nsc/infosharing/index.html

9/11 Recommendations Act
www.govtrack.us/congress/bill.xpd?bill=h110-1

MEMA
www.mema.state.md.us

WebEOC
www.esi911.com

CapWIN
www.capwin.org

RITIS
www.ritis.org

ICMA
icma.org

Law enforcement

National Center for Missing and Exploited Children
www.missingkids.com

Web-based Amber Alerts
www.codeamber.org/

National Information Exchange Model
www.niem.gov/

Suspicious Activity Report
www.occ.treas.gov/index.htm

National IEPD Clearinghouse
www.ncrnet.us/iepdclearinghouse

Public safety communication and interoperability

National Incident Management System
www.fema.gov/emergency/nims/index.shtm

National Public Safety Telecommunications Council
www.npstc.org/index.jsp

SAFECOM
www.safecomprogram.gov

Virginia Governor's Office of Interoperable Communication
www.interoperability.virginia.gov

PSIC grant information
www.ntia.doc.gov/psic/