



SECURITY NOTICE:

This is the redacted version of the Regional Critical Infrastructure Protection white paper/report.

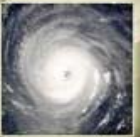
Based on current AHC policy, the full version of this white paper will only be made available to the following individuals:

- Regional Homeland Security Advisors
- Emergency Management Directors
- State Critical Infrastructure Protection Directors

For the public redacted version of the white paper, please visit www.ahcusa.org, and click on tabs for RESOURCES, then WHITE PAPERS.

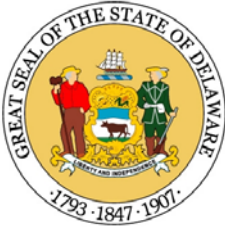


ALL HAZARDS CONSORTIUM



Mid-Atlantic Region

Critical Infrastructure Protection Workshop



Consortium States



Report Sponsored By:



Copyright © 2007

By All Hazards Consortium

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

Requests for permission to make copies of any part of the work should be mailed to:

Mr. Tom Moran, Executive Director
All Hazards Consortium Program Office
1600 Tysons Blvd
McLean, VA 22102

Printed in the United States of America.

Table of Contents

Message from the AHC Board of Directors on Process.....	1
Introduction.....	2
Key Issues.....	3
Summary of Discussion Topics.....	4
Recommendations.....	9
Conclusion.....	12

Message from the AHC Board of Directors on Process

The All Hazards Consortium (AHC) is a public-private partnership of Mid-Atlantic states and private corporations and utilizes a unique process to generate discussion on regional preparedness in the areas of homeland security and emergency management. This is accomplished by facilitating dialogue among state government leadership and interaction between AHC stakeholders. The AHC plans and implements one-day regional workshops that are hosted by the various states within the region.

At these workshops, multiple states come together to discuss common needs, problems, goals, and possible solutions in a variety of areas including policy, funding, technology and staffing. These requirements are captured by a combined AHC and private sector working group, which later reconvenes to vet the notes and produce a draft “report” that captures critical information and recommendations for going forward.

AHC Board of Directors

<i>President</i>	<i>Vice-President</i>
Robert Crouch Virginia	Evalyn Fisher Pennsylvania
<i>Secretary</i>	<i>Treasurer</i>
Dr. David Lindstrom Penn State University	Jim Spears West Virginia
Gordan Johnson New Jersey	Jackie Wasni Motorola
Darrell Darnell Washington, D.C.	Brian Darmody University Maryland
Andy Lauland Maryland	

AHC Advisory Committee

John Contestabile
Chairperson
Maryland

Chris Essid
Chairperson
PSCI Working Group
Virginia

Bud Mertz
Chairperson
CIP Working Group
Pennsylvania

Rich Kelly
Chairperson
IS&I Working Group

Tom Moran
Executive Liaison

Introduction

The All Hazards Consortium (AHC) supported the Critical Infrastructure Protection (CIP) Workshop hosted by Penn State University on October 3-4, 2007. The workshop convened over 100 attendees, including key personnel and stakeholders from the Federal government, the US military, the National Capital Region, non-governmental and private sector partners, and several Mid-Atlantic region and neighboring states, including Pennsylvania, Maryland, Virginia, Delaware, New Jersey, New York, Ohio, Kentucky, Tennessee, West Virginia, and South Carolina.

The workshop was designed to accomplish the following objectives:

- Provide a forum in which the region's Homeland Security Advisors and Critical Infrastructure Program leaders could conduct an open exchange of ideas related to CIP
- Further strengthen the CIP strategies for each state and the region
- Identify potential regional multi-state efforts
- Share best practices and lessons learned

This report highlights the recurring themes and issues discussed during the workshop and provides follow-on recommendations.

Critical Infrastructure Protection Background

The USA PATRIOT Act of 2001 defines critical infrastructure (CI) as assets "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating

impact on security, national economic security, national public health or safety." Historically, these assets have encompassed the following sectors:

- Transportation
- Water Systems
- Telecommunications
- Chemicals and Hazardous Materials
- Energy
- Public Health
- Emergency Services
- Defense Industrial Base
- Agriculture
- Banking and Finance
- Information Technology
- Postal and Shipping

Since CIP is the practice of securing these assets from man-made or naturally occurring disasters, it is essential for Federal, State, and local governments to craft strategies aimed at protecting sites from or making sites more resilient against many potential threats. As such, developing integrated CIP plans requires all levels of government to engage nonprofits, universities, research institutes, and the private sector in a collaborative dialogue that creates sustainable, trusting, security-focused relationships.

The AHC CIP Workshop is one step toward creating lasting partnerships that extend across the public-private divide and between states.

Key Issues

The workshop revealed that while states have made progress advancing CIP programs, some challenges remain.

Presently, most states are investing their limited resources into CI data collection and categorization. Some states have moved beyond data collection and have begun to analyze the data in meaningful ways. Specifically, an underpinning of CIP is risk management. States must be able to apply CI data, including the results of vulnerability assessments, to the development of state-wide risk profiles and assessments. This, in turn, would help them prioritize CI protection and identify necessary CI preparedness capabilities.

Robust risk assessments are essential to CIP since these assessments will drive the most beneficial use of Federal dollars. However, states require more robust funding and guidance for obtaining and developing the tools and methods to complete these risk assessments.

Second, issues related to the sharing sensitive information need to be addressed. The information sharing challenge is especially pertinent to how information is shared by the Federal government with state, local, and private sector entities and subsequently how states share that information with their partners. States must ensure that fusion

centers are actively engaged with CIP partners so that state-wide CIP information can be incorporated into risk assessments and subsequent analyses. Further, states must continue to engage in intra- and inter-state partnerships, as well as Federal partnerships.

Third, governance, policy, and technological improvements that support cross-jurisdiction, cross-state, and cross-sector interoperability help states overcome some information sharing barriers. However, overcoming existing technology challenges, such as database management and design, data security and access, and reporting protocols are needed.

Finally, a reallocation of resources between the states and localities should be considered in order to dedicate more funds to state-wide initiatives such as CIP.

It is clear that many of these challenges require a collective effort dedicated to resolving these issues across all levels of government. The Federal government and the States should continue to actively engage and receive endorsement from the private sector and coordinate with the states' 17 Critical Infrastructure/Key Resources (CI/KR) communities to promote an all-government/all-sector collaboration for CIP while remaining sensitive to privacy issues.

Summary of Discussion Topics

The AHC CIP Workshop afforded state CIP leaders and regional partners the opportunity to share their current status, challenges, needs, and best practices related to critical infrastructure protection in their respective states. Ten Mid-Atlantic States and the National Capital Region briefed workshop participants on the following topics:

- Critical Infrastructure Vision/Plan
- CIP Implementation
- Tools
- CIP Integration with Intelligence
- Information Technology
- Cyber Security
- Regional/Federal Interoperability
- Private Sector Involvement
- Best Practices and Lessons Learned

Discussion summaries from each of these topic areas are highlighted below. The following matrix displays the current status of CIP programs and implementation initiatives in each state.

	DC	DE	MD	NJ	NY	OH	PA	SC	VA	WV
CIP Plan	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Federal Funding	Y	Y	N	Y	Y	Y	Y	Y	Y	N
State Funding	N	N	N	Y	Y	N	N	N	Y	N
CIP Fusion Center	Y	Y	N	Y	Y	Y	N	Y	Y	Y
PCIII Accredited	N	N	Y	N	N	N	N	N	Y	N
Working Group Participation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Private Sector Outreach	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Database	ACAMS	None	None	DSB SP®	ACAMS	ACAMS	PA-specific	DSB SP®	ACAMS	HLS-CAM

CI Vision/Plan: State briefs described similar CI visions and implementation plans. These visions and plans collectively suggest that the process of critical infrastructure protection encapsulates an information sharing system that is sustained by trusting relationships and promotes methodologies that allow states to utilize CI data for making sound investments in the state’s preparedness.

Participants expressed a desire and a need to coordinate state resources into a risk-based CIP system that supports efficient CI data collection and analysis and interoperable CI information sharing. Outputs from such a risk-based system would drive the implementation of actual CIP measures and the development of other preparedness capabilities.

Participants recognized that implementing this vision is assisted greatly by intra- and inter-state partnerships which facilitate information sharing among and within state government and private sector entities. Standard procedures to share and protect sensitive and proprietary information can help establish such

partnerships and trusting relationships. Further, as additional information sources contribute to CI data, subsequent risk assessment and preparedness efforts will be more comprehensive and effective at achieving the overarching CI goal of ensuring the protection and resiliency of the state's critical infrastructure.

CIP Implementation: AHC member states have established a variety of governance structures to organize and coordinate CIP efforts. These efforts most often are federally funded with mandated funding split between localities and the state.

Presently, only two states are using State funds and resources to supplement federal funding for CIP efforts, which makes interoperability within states and between state governance structures paramount. That is, without adequate, sustained funding, states must maintain clear and reliable ways to communicate and work together to leverage, share, and pool limited resources. Additionally, until more funding from the Federal government is secured, state governance structures must be able to coordinate with each other, as well as with the private sector, to identify more effective ways to implement CIP strategies.

Workshop participants also discussed CI information challenges faced while implementing CIP visions. Each state develops several CI lists which need to be continuously tracked, coordinated, vetted, validated, and sustained. These list maintenance efforts become increasingly difficult as the number of CI lists in each state multiplies.

Furthermore, as CI lists become finalized, participants reported the need for more resources to fully adopt technologies that provide protocols, methods, and algorithms for analyzing

CI data. Such technologies would allow states to create state-wide risk profiles and conduct risk assessments, which could then be linked to response capabilities and resource allocation decisions.

Tools: The process of collecting and analyzing CI information is one that requires time, resources, and diligence. Workshop briefs revealed that each state employs unique methods and techniques for creating, categorizing, and consolidating state-wide CI lists. Similarly, states utilize various technological tools, such as ACAMS and Digital Sandbox Inc. (DSI) Site Profiler®, to assist in data collection and subsequent assessment/analysis efforts.

The discussion suggested that the variety of data collection methods and tools is a function of state-specific needs, financial circumstances, and resource allocations.

Participants agreed that for the CI data collection and assessment/analysis process to be most effective, specific data requirements must be defined to support the selection of the technology used for assessments and analyses, rather than allowing technologies to drive assessments and analyses. Thus, it is important that states select and utilize tools based on their specific data and analysis requirements while also ensuring that the selected tools are interoperable with other technologies used within the region.

CIP Integration with Intelligence: Workshop briefs revealed that some form of a fusion center has been developed in most states. Workshop participants reported that many sources, including Federal, inter-state, state, local, and private sector partners, contribute information to the fusion centers.

While fusion centers clearly must play a role in vetting, coordinating and fusing information into actionable intelligence, states continue to clarify the overall policies, function, mission, and responsibilities of the centers.

As fusion center operating concepts continue to develop, workshop briefs indicated that they also require an interface with state and local CIP programs. Workshop participants universally identified the need for bi-directional information flow and IT interoperability between state fusion centers and CIP efforts. Many states indicated that CIP/Intel working groups, comprised of a wide-range of stakeholders, can facilitate such bi-directional information flow.

Information Technology: Maintaining interoperable, sustainable computer information systems, represented on a common platform and backed by standard operating procedures, is a key requirement of cataloguing, retrieving, and sharing CI information among appropriate stakeholders.

First, discussion revealed that state and local agencies need interoperable software packages that seamlessly input and transmit data among agencies and private sector partners reduce duplication, maximize resources, and enhance increase information sharing and collaboration efforts.

Second, participants also determined that clearly defined protocols for managing and reporting changes to CI information must be established. Third, data collection and information centers must be staffed to ensure the accurate and secure, yet unimpeded flow of actionable CI information.

Finally, underpinning these issues is the need to secure steady funding streams.

Adequate and reliable funding will promote the development of properly manned, interoperable IT systems that facilitate collaboration across multiple jurisdictions and sectors.

Cyber Security: Protecting computer and data processing assets from unauthorized access or leaks is the hallmark of an effective cyber security strategy. Designing a plan to protect information related to CI plans, procedures, and vulnerabilities, as well all sensitive electronic information, requires not only secure information systems, but clearly defined processes and authentication protocols for sharing sensitive data across public-private sectors.

The workshop revealed the need for a common definition of cyber security. That is, some states view cyber security as a technical requirement to prevent the illicit distribution of sensitive electronic information and to promote a sense of comfort among state and regional partners engaged in information sharing with the state government. Others view the cyber world as a piece of critical infrastructure itself, which if compromised, potentially would have debilitating effects on state functioning and stability. A common definition of cyber security—and the government’s role in it—must be defined to align and coordinate efforts moving forward.

Nonetheless, participants agreed that cyber security is an overarching CI issue. Workshop participants determined that cyber security can be addressed through a variety of mechanisms, such as incident response teams and public-private advisory groups that identify industry and region-specific security requirements. State participants also agreed that cyber vulnerability assessments should be conducted on a joint-basis, bringing together

government and industry expertise so threat information can be properly leveraged. Many states reported that most efforts, thus far, have focused on protecting government systems from cyber attack.

To address concerns, some states indicated that highly sensitive pieces of information are distributed on a need-to-know basis to reduce the chances of electronically distributed information being acquired through illicit means.

Interoperability: Properly assessing and preparing for regional events involving critical infrastructure requires states and the private industry to possess tools and processes that facilitate information sharing among contiguous states and across jurisdictions.

The workshop revealed that creating interoperable data collection systems that integrate region and sector-specific information could assist stakeholders in assessing shared vulnerabilities and threats against critical sites. Additionally, such tools would help first-responders and key decision-makers respond to—and allocate resources toward—catastrophic events both within and across state lines.

Workshop participants indicated that establishing Memorandums of Understanding / Memorandums of Agreement (MOUs / MOAs) between states is crucial to promoting interoperability. Such agreements could assist border states in developing coordinated, multi-district approaches to mitigating natural or man-made CI incidents.

Additionally, many agreed that states should pursue Protected Critical Infrastructure Information (PCII) accreditation. The PCII program was developed to encourage industry

partners to share information with government officials by ensuring such data would not be disclosed to unauthorized sources.

Closely related, both the private sector and state representatives should consult their Protection Security Advisors (PSAs) more often to discuss additional security measures. DHS should provide greater understanding of the role and resources that PSAs can offer to states as they implement their CIP initiatives.

Private Sector Involvement: Trusting and sustainable relationships with the private sector form the backbone of any collaborative CIP plan. As such, Federal, state, and local governments should encourage both public-private and private-private outreach programs that eliminate barriers to information sharing.

AHC member states determined that governments can better incorporate private industry into CIP by developing public-private working groups that inform commercial and government officials of best practices and appropriate security measures related to CIP. Similarly, encouraging the formation of sector-specific committees within the private sector could assist owners and operators in devising plans that could prevent or protect against CI incidents. States and private industry may also benefit from incorporating elements of the private sector into fusion center operations. Maintaining a private sector presence at fusion centers could assist decision-makers integrate industry-specific information into multi-source assessments of CI threats and vulnerabilities. Furthermore, private sector participation in fusion centers and related CIP programs could strengthen public-private dialogue, and enhance the proper and responsible sharing of information between each sector.

Best Practices and Lessons Learned:

During the workshop participants shared the best practices and lessons learned in their respective states. While states are experiencing many successes in their CIP efforts, some of the most notable best practices and lessons learned suggest:

- Face-to-face contact and interaction with the private sector to promote CIP partnerships.
- Intel systems which routinely share information with different municipalities.
- Central CIP point of contact repositories available for efficient CIP collaboration.
- Regional, intra- and inter-state working groups and conferences which promote CIP initiatives.
- Sector-specific working groups which contribute to a state's overall CIP effort.
- Suspicious activity reporting systems which use threat information and statistical analyses to identify potential CI threats.
- Jurisdictional fusion centers which are linked to the State fusion center to promote CI and Intel information sharing.
- PCII accreditation to facilitate information sharing at all levels of government.
- Information sharing protocols that promote the sharing of sensitive information on a need-to-know basis.

Recommendations

Each day, workshop activities concluded with a discussion highlighting common themes and regional needs discussed during the day. Participants identified the following recurring issues which require further attention and action by AHC members, states, and partners.

1. Transition from CI list management to CI risk management. Workshop participants indicated that significant amounts of time and resources are devoted to CI data collection and CI list management.

Discussions highlighted the need to begin looking beyond CI list management and toward the assessment and application of the information collected. Thus, participants agreed that a risk-based CIP management system which includes protocols, methods, and algorithms for utilizing and prioritizing CI data for preparedness and protection purposes is necessary. Such a system would enable states to conduct risk assessments and analyses, which then could be linked to preparedness capabilities within a greater risk management program.

Action Items:

- Seek assistance at the regional and state level in developing risk assessment methodology which:
 - facilitates the use of already collected CI data
 - helps establish a preparedness risk management program
 - assists in the determination of preparedness capability requirements
 - takes into consideration current state and local risk assessment efforts.

2. Incorporate threat information into risk assessments. As states begin to conduct risk assessments, participants agreed that they should identify ways to incorporate the dynamic quality of threat information into their assessments.

Action Items:

- Further refine the role of the fusion center regarding the integration of intelligence and CI information.
- Create a regional risk-based CIP system to link intelligence and CI information to regional risk.

3. Establish clear performance metrics for CIP programs. Workshop participants agreed that preparedness is a difficult concept to measure. Oftentimes, what states believe to constitute CIP preparedness actually may not provide or represent the capabilities necessary to ensure the protection and resiliency of CI. Thus, states need a way to assess the viability of their efforts and programs. Workshop participants recognized the benefit of a self-assessment tool with tangible and valid performance metrics against which they could gauge and measure their CIP capabilities.

Action Items:

- Consider the Target Capability List (TCL) when developing CIP metrics.
- Based on an assessment of the TCL, begin developing performance measures that align with state-specific risks and the costs related to mitigating those risks.

4. Consider how “soft targets” should be incorporated into CIP efforts. Workshop discussion focused exclusively on “hard” CI targets, such as bridges,

railways, and ports. Participants suggested that their CI plans and visions should expand to include, or at least consider, “soft targets” such as hotels, churches, and commercial districts.

Action Items:

- Offer soft target awareness training to CIP personnel and private sector partners at the state level, or encourage participation in the Soft Target Awareness courses offered by DHS.
- Consider the displacement effect of target hardening and identify which targets in each state will become more vulnerable as CIP efforts increase.
- Incorporate soft target intelligence into risk management programs in order to adjust tactical and operational capabilities according to current potential threats.

5. Coordinate Federal initiatives across sectors. In addition to the Department of Homeland Security, several Federal agencies fund, contribute resources to, and/or participate in state CIP efforts. Each Federal agency maintains different rules and procedures for obtaining Federal assistance for CIP initiatives and supports different CIP programs. Workshop discussions suggested that these Federal initiatives be coordinated across the different sectors to maximize the efficiency of limited resources.

Action Items:

- Ensure Federal collaboration with the states to represent a unified CI voice.
 - Compare the state CIP initiatives outlined in this white paper with Federal CIP strategies and advocate for Federal

initiatives that align best with state initiatives.

- To promote an all-government/all-sector collaboration for CIP, provide an opportunity for the private sector to comment on the states’ efforts to align state and Federal CIP strategies.
- Distribute AHC white papers to lawmakers and government officials to increase awareness of ongoing CIP efforts, needs, and challenges.
- Educate lawmakers and government officials on the interconnectivity of all CI sectors and the necessity to promote universal, rather than sector-specific, CIP efforts.

6. Secure CIP funding. The majority of states reported that their CIP efforts rely solely on Federal funding. Participants suggested that the AHC and CIP stakeholders contact and develop relationships with lawmakers and appropriators to request and ensure that funding is dedicated for CIP annually.

Action Items:

- Consider a reallocation of resources between the states and localities in order to dedicate more funds to state-wide initiatives such as CIP.
- Distribute AHC white papers to lawmakers and government officials to increase awareness of ongoing CIP efforts, needs, and challenges.

7. Promote public-public, public-private, and private-private partnerships. CIP relies on an information sharing system that is sustained by trusting relationships. Workshop participants agreed that face-to-face contact and regular interaction

with CIP partners at all levels is the best way to unite behind the common cause of ensuring the protection and resiliency of the region’s critical infrastructure.

Action Items:

- Engage in continual and ongoing collaboration efforts with fellow AHC members and partners by hosting and attending meetings, discussions, forums, workshops, and conference calls.
- Explore ways to use the annual summit meeting, the All Hazards Forum, as a way to continue to promote collaboration and CIP awareness.
- Continue to share best practices and lessons learned.

Conclusion

The AHC CIP Workshop was a successful event that allowed the vested and dedicated AHC members and partners to coordinate and share their CIP efforts. While participants discussed many issues and concerns, the following overarching objectives remain:

1. Secure additional funding dedicated to state CIP efforts.
2. Acquire adequate personnel to fulfill CIP needs.
3. Establish procedures and protocols to ensure information security.
4. Use CI data as a foundation for all-hazards risk management programs.

In addition to securing CIP-dedicated funding, consideration also must be given to the mandated allocation of Federal funds between the state and localities in each state. A larger allocation of Federal funding to states would allow them to implement state-wide initiatives such as CIP. As state CIP initiatives are implemented, states will be able to move from CI list management toward CI risk management and the development of preparedness risk management programs.

A united effort among AHC members, state representatives, Federal partners, private sector entities, and interested stakeholders must continue to strengthen partnerships across all levels of government. Such collaboration is important to achieving the CI goal of CI resiliency and protection.

About the All Hazards Consortium (AHC)

The AHC is a 501c3 organization governed by public/private sector members focused on regional state government homeland security and emergency management collaboration within the Mid-Atlantic Region. It was formed in 2003 by the states of Virginia, Maryland and the District of Columbia, the AHC was formed to provide a framework to engage business, higher education R&D, and state and local government to share problems and solutions. Membership has grown to include the member states of NC, VA, WV, DC, MD, DE, PA, NJ and NY. Today the AHC serves as a means for member states to focus on solving problems at a regional level, building on trust relationships and common need. For more information visit www.ahcusa.org.

About CNAC

The CNA Corporation (CNAC) is a non-profit research organization that operates the Center for Naval Analyses and the Institute for Public Research. Through innovative analysis, CNAC provides public sector organizations with the tools to tackle complex problems. CNAC's objective, empirical research and analysis help decision makers form sound policies, make better informed decisions, and manage programs more effectively. In so doing, CNAC has established itself at the forefront of efforts to make our country safer and stronger, and our government more efficient. The organization is defined by a unique brand of multi-disciplinary, field-based "real world" research and analysis.

Special Thanks

The AHC would like to extend a special thanks to Pennsylvania State University for hosting and facilitating this successful workshop and to the CNA Corporation for providing support for the development of this report. Thanks also to our other workshop sponsors and the AHC Partners:

CIP Workshop Hosts

David Lindstrom, Chief Privacy Officer, Penn State University

Jim Powers, Director for the Office of Homeland Security, Commonwealth of Pennsylvania

CIP Workshop Sponsors

Global Security Systems
Mogility Technology Corp
Digital Sandbox
SSI Services
All Hazards Forum / EJ Krause and Associates
Pennsylvania State University

Corporate Supporters

Motorola
TerreStar
Sprint
All Hazards Forum / EJ Krause and Associates
Verizon Business
Verizon Wireless
CISCO
M/A-Com
Lockheed Martin
The Artemis Group
MITRE
IBM
SAIC
Dutko Worldwide
Lucent Technologies
Smart & Associates
Integrity Consulting
CSC
Delcan Inc.
ITIS Holdings
CA Inc
Allstate
Northrop Grumman
CoreStreet
SES Americom
Intelsat General Corporation

State and Federal Presenters

Delaware: James Woznicki and Ronald Bounds, Delaware State Police

Department of Homeland Security: Colonel Bob Stephan, Assistant Secretary for Infrastructure Protection, Department of Homeland Security

Maryland: Lieutenant Kris Nelson, Maryland State Police

New Jersey: Joe Conrey, New Jersey Office of Homeland Security and Preparedness (NJ-OHSP)

New York: Brian Wright, Jaime Ian, and Mike Beckman, New York State, Office of Homeland Security

New York: Jon Duecker, New York Police Department

Ohio: Earl Mack, Ohio Department of Public Safety, Division of Homeland Security

Pennsylvania: Bud Mertz, Deputy Director for Critical Infrastructure Protection, Office of Homeland Security

South Carolina: Stephen G. Birnie, Office of the Homeland Security Advisor (HSA & SAA)

Virginia: Constance McGeorge, Governor's Office of Commonwealth Preparedness

Washington: DC: Steven Kral, Office Homeland Security and Emergency Management Agency

West Virginia: Ray Stonestreet, West Virginia State Police