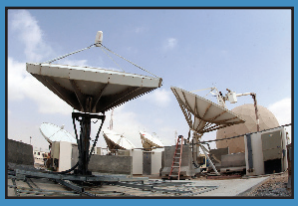
NDIA
National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

2009 DIB★CIP

DEFENSE INDUSTRIAL BASE CRITICAL INFRASTRUCTURE PROTECTION CONFERENCE & TECHNOLOGY EXHIBITION

"DIB RESILIENCY THROUGH PROTECTION, RESPONSE AND RECOVERY"



ONSITE AGENDA

MARCH 31-APRIL 3, 2009
WWW.NDIA.ORG/MEETINGS/9030 ▶ SAN ANTONIO, TX ▶ THE ST. ANTHONY WYNDHAM
EVENT #9030

TUESDAY, MARCH 31, 2009

12:00-6:30pm Registration

5:00-6:30pm Reception

WEDNESDAY, APRIL 1, 2009

7:00-8:00am Registration/Continental Breakfast

8:00-8:15am Welcome/Introduction

- *Mr. Antwane Johnson, Director, Defense Critical Infrastructure Program, OASD (HD&ASA)*

8:15-9:00am DoD/Government Keynote Address: "Examining the Threats to the Defense Industrial Base"

- *Dr. Joel F. Brenner, National Counterintelligence Executive and Mission Manager for Counterintelligence, Office of the National Counterintelligence Executive*

Dr. Brenner will provide an examination of threats, which could significantly impact the capabilities of the Defense Industrial Base.

9:00-9:45am Industry Keynote Address: "Maintaining Resiliency Within the Defense Industrial Base Through Preparedness, Response and Recovery"

- *Mr. Dave Komendat, Chief Security Officer, The Boeing Company*

Mr. Komendat will address the complex issues associated with developing and executing enterprise-wide resiliency plans and capabilities. There are specific challenges to maintaining an "integrated management system." These include continuity of business operations, physical security, accountability of key personnel, as well as cyber and supply chain security and effective information sharing strategies.

9:45-10:15am Break in Exhibit Hall

10:15-11:30am Information Sharing Panel: "The Information Sharing Environment – Technological Successes & Cultural Challenges"

Moderator:

- *Mr. Vincent Jarvie, Vice President, Corporate Security, L-3 Communications Corporation*

Panelists:

- *Mr. Mark Levett, Unit Chief, FBI HQ*
- *Mr. Tom Patterson, Founder, National Security Grid*
- *Mr. Robert "Jim" Caverly, Director, Partnership and Outreach Division, Office of Infrastructure Protection, DHS*

Since 9/11, information sharing has been aggressively promoted from the highest levels of government down to small towns and rural communities. In some circles, the term has become almost cliché. However, the fact remains that information needs to be shared to maintain the uninterrupted operation of government and private sector business. Information needs vary greatly and span across many areas. Whether faced with threats of terrorist acts or natural disasters, having access to pertinent critical information will greatly enhance the ability to coordinate response and recovery efforts between different agencies. The technologies that facilitate this type of information sharing exist but certain barriers still persist. Has the cultural shift actually been embraced? Have we fully transitioned from a "need to know" to a "need to share" mentality? This panel will focus on these and other issues facing the Information Sharing Environment today.

11:30-12:45pm Buffet Lunch in Exhibit Hall

12:45-2:00pm **Cyber Security Panel: "Defending Cyberspace – The Best Defense Is a Strong Offense"**

Moderator:

- *Mr. Steve Lines, Director of Business Continuity & Information Assurance, SAIC*

Panelists:

- *Mr. Steven Fullbright, Sr. Director, eBusiness Information Delivery & Security, Rockwell Collins, Inc.*
- *Mr. Joe Wassel, Deputy Director, Intelligence, Interagency and Networks, DIB Cyber Security Task Force*
- *Mr. Mike Gordon, CISSP, IAM/IEM, Senior Manger, Computer Incident Response Team (CIRT), Lockheed Martin Corporation*

In order to effectively protect our systems against Cyber Terrorism, we must understand the new, as well as persistent cyber threats. Cyber Security will always be a pressing issue. If networks are not monitored and frequently updated, the damage could be extensive. This panel will explore effective methods to deploy an in-depth defensive front line to reduce vulnerabilities and prevent network intrusions; know who is on your network; defend against the full spectrum of threats through the use of real time intelligence; identify cyber security solutions that can be shared across government and industries, and determine technology research development investment needs.

2:00-2:30pm Break in Exhibit Hall

2:30-3:45pm
3:45-5:00pm

Consecutive Breakout Sessions (Information Sharing/Cyber Security)

Breakout sessions will be held twice consecutively during the afternoon, giving attendees the opportunity to participate in both sessions.

Information Sharing Breakout Session

Facilitator:

- *Mr. Steven Kipp, Information Systems Security Manager, L-3 Communications Corporation*
- *Mr. Robert "Jim" Caverly, Director, Partnership and Outreach Division, Office of Infrastructure Protection, DHS*

There are multiple sources of information, all of equal importance to some but not to all. This will be the ideal forum for sharing success stories, as well as raising the prevalent issues affecting the ever evolving state of Defense Industrial Base sector resiliency across Federal, State, Local and Private Sectors, to include prime and subcontractors.

- *How can we ensure that the "right" information is getting to the "right" people?*
- *What are the newest technologies available, and are they scalable to the size, mission, and needs of our company and communities of interest?*
- *How can I know if sensitive proprietary information I am providing is protected from unauthorized dissemination?*
- *What happens to suspicious activity reports involving critical infrastructure facilities?*
- *Are the appropriate federal law enforcement agencies or local police departments being alerted for further response as appropriate?*

Cyber Security Breakout Session

Facilitators:

- *Mr. Steve Lines, Director of Business Continuity & Information Assurance, SAIC*
- *Mr. Joe Wassel, Deputy Director, Intelligence, Interagency and Networks, DIB Cyber Security Task Force*

Facilitators will guide participant discussion to develop actionable recommendations for improving threat identification & reporting, solution sharing, as well as new technology development.

- *What solutions can be implemented that will protect our computer systems against cyber terrorism?*
- *What are the Government and Department of Defense doing to address these threats?*
- *What is private industry observing, and how are they handling these threats?*
- *How can smaller businesses with limited financial resources effectively protect their systems in an affordable manner?*

5:00-6:30pm

Reception in Exhibit Hall

THURSDAY, APRIL 2, 2009

7:00-8:00am — Registration/Continental Breakfast

8:00-8:15am — Recap

- *Mr. Antwane Johnson, Director, Defense Critical Infrastructure Program, OASD (HD&ASA)*

8:15-9:00am — Keynote Address

- *Dr. Marc H. Siegel, Security Management System Consultant, ASIS International*

Dr. Siegel will discuss how to use new national and international standards as tools to enhance your organization's resilience. A soon to be published U.S. standard for Organizational Resilience Management can be used to address many of the major issues that we must overcome to achieve organizational resiliency in a cost effective way. Dr. Siegel will also provide an update on the state of the ISO 28000 series of standards for Supply Chain Security and evolving efforts to further improve the national and international standards dealing with security and resilience of the supply chain.

9:00-9:45am — Keynote Address

- *MG Vincent E. Boles, USA, Assistant Deputy Chief of Staff, G4*

MG Boles will discuss the framework to help maintain acceptable levels of risk throughout the DIB sector in working with Federal, regional, state, local, tribal, foreign governments, and non-governmental organizations. Defense Industrial Base Preparedness is a key aspect in managing risk to warfighting capabilities. Emphasis is placed on the importance of the public/private partnership between the federal government and defense contractors, their subcontractors, state, tribal, local governments and other sectors to develop preparedness plans in order to effectively respond and recover from major incidents. MG Boles will discuss success stories/best practices and challenges in developing and implementing preparedness plans for responding and recovering from major events.

9:45-10:15am — Break in Exhibit Hall

10:15-11:45am — Business Continuity Panel: "Business Continuity 101 – Foolproof Plans to Ensure Survivability"

Moderator:

- *Mr. Robert Connors, Preparedness Director, Raytheon Company*

Panelists:

- *Dr. Marc H. Siegel, Security Management System Consultant, ASIS International*
- *Dr. Edward Cahn, PMP, CBCP, Business Continuity Coordinator, BAE Systems*
- *Mr. Robert "Jim" Caverly, Director, Partnership and Outreach Division, Office of Infrastructure Protection, DHS*
- *Mr. Bob Irwin, Assistant Emergency Manager, Commander, Navy Region Southeast*

Building an effective business continuity plan is a multi-faceted process and "one size does NOT fit all." Private sector companies and DoD Government Owned Government Operated (GOGO) facilities must take proactive steps to ensure that their critical business functions remain operational and products and services are available to customers, suppliers and other entities. In order to accomplish this, they must be able to accurately assess their business continuity plan on a frequent basis. This session will talk about business continuity, best practices, and how to accurately assess the effectiveness of a business continuity plan.

11:45-12:45pm — Buffet Lunch in Exhibit Hall

12:45-2:00pm — **Supply Chain Security Panel: "Supply Chain Security – Recognizing Global Interdependencies & Creating a Trusted Environment"**

Moderator:

- *Mr. William Tate, Manager of Security for the Battle Management and Engagement Systems Division, Northrop Grumman Aerospace Systems*

Panelists:

- *Mr. Larry Clinton, President and CEO, IS Alliance*
- *Mr. Irvin Varkonyi, CSCP, Marketing Manager, Transportation and Logistics, American Public University*
- *Dr. Marc H. Siegel, Security Management System Consultant, ASIS International*

A panel aimed at combining current research with industry security practices and identifying challenges in global supply chain management, particularly the security management. The follow on breakout session will strive to examine factors that result in a healthy supply chain and identify major factors that influence supply chain risk decisions.

2:00-2:30pm — Break in Exhibit Hall

2:30-3:45pm
3:45-5:00pm — Consecutive Breakout Sessions (Business Continuity/Supply Chain Security)

Breakout sessions will be held twice consecutively during the afternoon, giving attendees the opportunity to participate in both sessions.

Business Continuity Breakout Session

Facilitators:

- *Mr. Scott McCoy, Chief Security Officer, Alliant Techsystems (ATK)*
- *Mr. Bob Irwin, Assistant Emergency Manager, Commander, Navy Region Southeast*

This session will identify industry challenges, best practices and guidelines for building, maintaining and exercising continuity of business operations plans for large, medium and small business at affordable cost. Methods for risk management, business impact analysis, business continuity strategy and plan development, and testing and maintenance of plans are the basis for discussion, taking existing private sector policies, guidelines, standards, procedures and best practices into consideration. After attending this session, you will walk away with viable solutions and best practices based on lessons learned within the Defense Industrial Base.

- *What are the top two strategic and tactical business continuity planning challenges?*
- *What specific actions can be taken by government and industry to address each challenge?*
- *How can we accurately identify our critical functions?*
- *What can be done to build a trusted environment, which adheres to the same standards?*
- *Is our plan scalable?*
- *How can we test our present business continuity plan to know that it will be effective?*
- *Is our current business continuity plan accounting for critical personnel, as well as assets?*

Supply Chain Security Breakout Session

Facilitators:

- *Mr. William Tate, Manager of Security for the Battle Management and Engagement Systems Division, Northrop Grumman Aerospace Systems*
- *Mr. Irvin Varkonyi, CSCP, Marketing Manager, Transportation and Logistics, American Public University*

The session will discuss methods to construct, implement and justify an effective supply chain risk management strategy/plan. Facilitators will challenge participants to identify and share knowledge about tools and best practices that identify and prioritize critical business elements, mapping the entire supply chain to show interdependencies, and identify potential failure points along the supply chain.

- *How can we be sure that our company is equipped to provide a constant flow of goods and services during a crisis?*
- *What security risk management plans have been implemented by other companies within the Defense Industrial Base and which ones have been successful?*
- *How are Government Agencies in the Defense Industrial Base dealing with this?*
- *What are the long-term foreseen security challenges?*

5:00pm Exhibit Hall Closes

FRIDAY, APRIL 3, 2009

7:00-8:00am Registration/Continental Breakfast

8:00-8:15am Recap

- *Mr. Antwane Johnson, Director, Defense Critical Infrastructure Program, OASD (HD&ASA)*

8:15-9:00am — Keynote Address

- *Senior FEMA Executive (TBD)*

FEMA will address emergency management planning and the actual experience, observations and lessons learned from responding and recovering from a major catastrophic event in coordination with federal, state and local governments, and the private sector.

9:00-9:45am — Keynote Address: "Preparing, Responding & Recovering from a National Emergency"

- *Mr. Steve McCraw, Texas Homeland Security Director, Office of the Governor*

Mr. McCraw will share the experiences of successfully engaging with incident planning and response stakeholders (private companies, local responders, local, state, tribal and federal governments) to successfully plan, coordinate, respond and recover from major events such as Hurricane Ike. In particular, he will highlight what worked well and what areas could be improved upon in the process. Ideas to improve the preparedness planning and response process will be shared.

9:45-10:00am — Break

10:00-10:45am — Compilation/Debriefing of Breakout Session Facilitator Reports

10:45-11:00am — DoD Closing Remarks

11:00am — Conference Adjourns