Files are in Adobe format.
Download the newest version from Adobe.

2011 Defense Industrial Base Critical Infrastructure Protection Conference (DIBCIP)

"Setting the Vision and Strategy for the Next Decade"

August 23-25, 2011
Philadelphia, PA

Agenda

Supplemental Materials

Wednesday, August 24, 2011

AN INDUSTRY PERSPECTIVE ON THE INFORMATION SHARING ENVIRONMENT OF 2020
- Ms. Chandra McMahon, Vice President and Corporate Information Security Officer, Enterprise Business Services, Lockheed Martin Corporation

INFRASTRUCTURE DEPENDENCIES: THE BIG ROCKS PANEL
Moderator: Mr. Robert B. Stephan, Former Assistant Secretary for Infrastructure Protection, DHS
- Mr. Guy Copeland, Vice President, Information Infrastructure Advisory Programs and Special Assistant to the CEO, CSC

Thursday, August 25, 2011

INFORMATION SHARING PANEL
Moderator: Mr. Tom Watson, Director, Infrastructure Coordination and Analysis Office, DHS
- Mr. William D. Stephens, Director, Counterintelligence, Defense Security Service
- Mr. Michael Howell, Deputy Program Manager, Office of the Program Manager, Information Sharing Environment

ENGAGEMENT IN PREPAREDNESS RESILIENCY PANEL
Moderator: Mr. Robert Read, Senior Industrial Analyst, OSD AT&L MIBP
- Mr. John Guest, IP Regional Director, Mid-Atlantic Region, Protective Security Advisor, DHS
- Mr. Jerry Middleton, Vice President, Corporate Development, Elusys Therapeutics, Inc.
- Mr. Theodore M. Davidson, Security and Emergency Services Leader, ULA
- Ms. Cherrie Black, Bureau Chief, Critical Infrastructure Protection Bureau, New Jersey State Office of Homeland Security and Preparedness

THE FUTURE OF RESPONSE, RECOVERY AND RECONSTITUTION CAPABILITY PANEL
Moderator/Panelist: Mr. Richard Irwin, Vice President, Homeland Security and the Intelligence Community, MELE Associates
- Mrs. MaryAnn Tierney, FEMA
- Dr. Thomas Bogdan, Director of the Space Weather Prediction Center, NOAA, DoC

NDIA
National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

2011 DIB ★ CIP

DEFENSE INDUSTRIAL BASE CRITICAL INFRASTRUCTURE PROTECTION CONFERENCE

"Setting the Vision and Strategy for the Next Decade"

AUGUST 23-25, 2011
EVENT #1030 ▶ PHILADELPHIA, PA ▶ SHERATON SOCIETY HILL HOTEL
WWW.NDIA.ORG/MEETINGS/1030

TUESDAY, AUGUST 23, 2011

12:00pm-6:30pm — **Registration**
Society Hill Ballroom Foyer

5:00pm-6:30pm — **Opening Networking Reception**
Society Hill Ballroom AB

WEDNESDAY, AUGUST 24, 2011

7:00am-5:00pm — **Registration**
Society Hill Ballroom Foyer

7:00am-8:00am — **Continental Breakfast**
Society Hill Ballroom AB

8:00am-8:15am — **Welcome & Introductory Remarks**
Society Hill Ballroom CDE
- MG Barry D. Bates, USA (Ret), Vice President, Operations, NDIA; DIB SCC Chairman

8:15am-9:00am — **Government Keynote Address (DoD)**
Society Hill Ballroom CDE
- Mr. Jose Mayorga, DASD Strategy, Force Planning and Mission Assurance, OASD HD&ASA

9:00am-9:45am — **Government Keynote Address (DHS)**
Society Hill Ballroom CDE
- Mr. Todd M. Keil, Assistant Secretary, Infrastructure Protection, DHS

9:45am-10:15am — **Joint Question & Answer Session**
Society Hill Ballroom CDE
- Mr. Jose Mayorga, DASD Strategy, Force Planning and Mission Assurance, OASD HD&ASA
- Mr. Todd M. Keil, Assistant Secretary, Infrastructure Protection, DHS

10:15am-10:30am — **Networking Break**
Society Hill Ballroom Foyer

10:30am-12:00pm — **Industry Keynote Panel**
Society Hill Ballroom CDE
Moderator: Mr. Charles Kosak, Principal Director, Homeland Defense Strategy, Force Planning & Mission Assurance, OASD HD&ASA

- Mr. Irwin F. Edenzon, Corporate Vice President, Huntington Ingalls Industries; President, Ingalls Shipbuilding
- Mr. John Jolly, Vice President and General Manager, Cyber Systems Division, General Dynamics Advanced Information Systems

12:00pm-1:15pm — **Networking Lunch**
Society Hill Ballroom AB

1:15pm-2:00pm — **An Industry Perspective on the Information Sharing Environment of 2020**
Society Hill Ballroom CDE
- Ms. Chandra McMahon, Vice President and Corporate Information Security Officer, Enterprise Business Services, Lockheed Martin Corporation

2:00pm-3:15pm — **DIB Cyber Mission Assurance Panel**
Society Hill Ballroom CDE
Moderator/Panelist: Mr. Robert J. Giesler, Senior Vice President, Cyber Programs, SAIC

- Mr. Brendan Goode, Director of Network Security Deployment, National Cyber Security Division (NCSD), DHS
- Mr. Carlos Solari, Vice President, Cyber Technology and Services, CSC

Purpose: Provide a brief introduction to DoD cyber mission assurance policy. Present and discuss current challenges to staying ahead of cyber adversaries and how well we're doing; what new challenges the next decade may bring and what the 2020 cyber world may look like for the DIB.

3:15pm-3:45pm — **Networking Break**
Society Hill Ballroom Foyer

3:45pm-5:00pm — **Infrastructure Dependencies: The Big Rocks Panel**
Society Hill Ballroom CDE
Moderator: Mr. Robert B. Stephan, Former Assistant Secretary for Infrastructure Protection, DHS

- Mr. Guy Copeland, Vice President, Information Infrastructure Advisory Programs and Special Assistant to the CEO, CSC
- Mr. Douglas Ochsenknecht, Mission Assurance Division Head, NSWC Dahlgren
- Mr. Brandon Wales, Director, Homeland Infrastructure and Risk Analysis Center (HITRAC), DHS

▶ Brig Gen James Muscatell, Mobilization Assistant to USTRANSCOM J3, USTRANSCOM Operations & Plans

Purpose: Discuss new developments that have improved our understanding about the interdependencies among the Energy, Communications and Transportation sectors with particular emphasis on the electric power grid. Explore unresolved and emerging issues that must be resolved in this decade. Discuss what "big rock" infrastructure interdependency questions may remain unanswered in 2020.

5:00pm **Adjourn for the Day**

THURSDAY, AUGUST 25, 2011

7:00am-12:15pm **Registration**
Society Hill Ballroom Foyer

7:00am-8:00am **Continental Breakfast**
Society Hill Ballroom AB

8:00am-8:05am **Welcome & Introductory Remarks**
Society Hill Ballroom CDE
▶ MG Barry D. Bates, USA (Ret), Vice President, Operations, NDIA; DIB SCC Chairman

8:05am-9:30am **Information Sharing Panel**
Society Hill Ballroom CDE
Moderator: Mr. Tom Watson, Director, Infrastructure Coordination and Analysis Office, DHS

▶ Mr. William D. Stephens, Director, Counterintelligence, Defense Security Service
▶ Mr. Michael Howell, Deputy Program Manager, Office of the Program Manager, Information Sharing Environment
▶ Mr. Vince Jarvie, Vice President, Corporate Security, L-3 Communications Corporation

Purpose: Present a brief retrospective on advances in interpersonal, physical and technological information sharing across all levels of government and the private sector. Discuss the top three information sharing issues that must be resolved in this decade and how that will provide a springboard for further advancements beyond 2020. How can classified information with DIB partners be economically and effectively shared without compromising security?

9:30am-9:45am **Networking Break**
Society Hill Ballroom Foyer

9:45am-11:00am **Engagement in Preparedness Resiliency Panel**
Society Hill Ballroom CDE
Moderator: Mr. Robert Read, Senior Industrial Analyst, OSD AT&L MIBP

- Mr. John Guest, IP Regional Director, Mid-Atlantic Region, Protective Security Advisor, DHS
- Mr. Jerry Middleton, Vice President, Corporate Development, Elusys Therapeutics, Inc.
- Mr. Theodore M. Davidson, Security and Emergency Services Leader, ULA
- Mr. Richard Fortson, Jr., Physical Security Leader, Production Operations, ULA
- Ms. Pamela Kuczek, Risk Manager, ULA
- Ms. Cherrie Black, Bureau Chief, Critical Infrastructure Protection Bureau, New Jersey State Office of Homeland Security and Preparedness

Purpose: Discuss a case study for a local small business fully engaged in supporting national defense and how state and local governments facilitate preparedness against the spectrum of threats and hazards that could disrupt or destroy the productive capability of the business.

11:00am-12:15pm **The Future of Response, Recovery and Reconstitution Capability Panel**
Society Hill Ballroom CDE
Moderator/Panelist: Mr. Richard Irwin, Vice President, Homeland Security and the Intelligence Community, MELE Associates

- Mrs. MaryAnn Tierney, FEMA
- Mr. Clark Lystra, Defense Support of Civil Authorities, OASD HD&ASA
- Mr. Mike Smith, Director, Global Initiatives, Global Initiatives Directorate, Infrastructure Security and Energy Restoration Division, Office of Electricity Delivery and Energy Reliability, DoE
- Dr. Thomas Bogdan, Director of the Space Weather Prediction Center, NOAA, DoC

Purpose: Provide a brief retrospective leading to a discussion about what major changes the DIB and American society will observe before 2020 in the capability of national, regional, state and local response and recovery to catastrophic events. Discuss the “response and recovery” circumstances that may require

a resilient DIB to participate as a full partner with DoD and other national authorities, state and local government, and NGOs in capability reconstitution.

12:15pm

Closing Remarks
Society Hill Ballroom CDE
▶ Mr. Jose Mayorga, DASD Strategy, Force Planning and Mission Assurance, OASD HD&ASA

ATTIRE
Appropriate dress for the conference is business casual for civilians and class B uniform or uniform of the day for military personnel.

ID BADGE
During conference registration and check-in, each Attendee will be issued an identification badge. Please be prepared to present a valid picture ID. Your badge must be worn at all conference functions.

PROCEEDINGS
Proceedings will be available on the web through the Defense Technical Information Center (DTIC) two weeks after the conference. All registered Attendees will receive an email notification once the proceedings are available.

SPEAKER DONATION
In lieu of Speaker gifts, NDIA has made a donation to the Wounded Warrior Project.

For additional information, please visit:
www.woundedwarriorproject.org

SURVEY
A survey will be e-mailed to you after the conference. NDIA would greatly appreciate your time in completing the survey to help make our event even more successful in the future.

ADVERTISING
Advertise in *National Defense* magazine and increase your organization's exposure. *National Defense* will be distributed to Attendees of this event, as well as other NDIA events. For more information, please contact Mr. Dino Pignotti, NDIA, at (703) 247-2541 or dpignotti@ndia.org.

LOCATION
Sheraton Society Hill Hotel
One Dock Street
Philadelphia, PA 19106
(215) 238-6000

CONTACT
Ms. Brant Murray, Meeting Planner, NDIA
(703) 247-2572
bmurray@ndia.org

THANK YOU TO OUR SPONSORS!

CACI

EVER VIGILANT

CACI is a multifaceted solutions provider for the Federal Government with over 13,700 employees located in approximately 120 offices around the world. Since its inception in 1962, CACI has been a proven innovator – combining visionary technology with outstanding client support to deliver comprehensive, practical solutions for an ever-changing world environment.

CACI services and solutions help our clients provide for national security, improve communications and collaboration, secure the integrity of information systems and networks, enhance data collection and analysis, and increase efficiency and mission effectiveness. To ensure thought leadership for today's security challenges, CACI facilitates distinguished symposiums and publications that provide solutions for the Federal Government and Industrial Base.

We are dedicated to continually providing superior services within the Critical Infrastructure Protection (CIP), Mission Assurance and Resiliency areas. Our technical and consultative support extends across the Federal landscape and into the private sector. CACI understands that threats and hazards to our nation's critical assets, supply chains and infrastructure are always present and continually evolving. CACI professionals work with our government partners at the technological and operational heart of their efforts to counter these dangers and ensure our nation's security.

CACI's website is www.caci.com.

THANK YOU TO OUR SPONSORS!

ICF International (NASDAQ:ICFI) partners with government and commercial clients to deliver professional services and technology solutions to a variety of markets, including: homeland security and defense; environment and infrastructure; energy and climate change; and health, human services and social programs. The firm combines passion for its work with industry expertise and innovative analytics to produce compelling results throughout the entire program life cycle, from research and analysis through implementation and improvement. Selected offerings include policy and program development and implementation, program management and performance measurement, cybersecurity and compliance, strategic communications and outreach, capital investment planning for resource allocation, and training and exercises to enhance preparedness. ICF provides management, analytical and technical consulting support to the DHS Office of Infrastructure Protection and its partners in their efforts to ensure that resources are applied where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats, or minimizing the consequences of terrorist attacks and other incidents. Since 1969, ICF has been serving government at all levels, major corporations and multilateral institutions. More than 3,500 employees serve these clients worldwide.

ICF's website is www.icfi.com.

State and Local Support for CI/KR Preparedness & Resilience

Cherrie Black, Chair, State, Local, Tribal & Territorial Government Coordinating Council

Bureau Chief, Infrastructure Protection, New Jersey Office of Homeland Security & Preparedness

Sector Partnerships and Preparedness

- Provide unique regional, state and local preparedness perspectives and programs
- Augment national programs with regional, state and local “ground truth”
- Tie the sectors into regional, state and local planning and preparedness programs.

State Sector Specific Activities

- Organize State Level Sector Working Groups for key sectors and sub-sectors

- Identify Sector/Sub-sector risks & priorities

- Focus on Sector priorities: NJ DIB Training (e.g., surveillance detection), key worker credentialing, information sharing and collaboration with State and local stakeholders.

Resilience

- Resilience is the ability of an asset, system or network to absorb a significant disruption and return to an acceptable state of functionality within an acceptable period of time.(RTO-RTA)

- Lifeline Sectors (Water, Communications, IT, Energy, Transportation) support all CIKR sectors. The resiliency of lifeline sectors is paramount.

The Goal

- Determine what is critical.
- Understand the dependencies and interdependencies of critical assets.
- Manage risk to:
  - Protect and deter if possible/reasonable;
  - Prioritize restoration of essential services;
  - Emphasize emergency response planning;
  - Mitigate economic impacts; and
  - Promote expeditious resumption of trade/commerce.

The takeaway….

DIB SECTOR: Your mission is national, your crisis is local.

Insure that Managers, Planners and Responders understand your requirements and know how to prioritize your needs.

Space Weather

Dr Thomas J Bogdan

Director, Space Weather Prediction Center
Boulder, CO

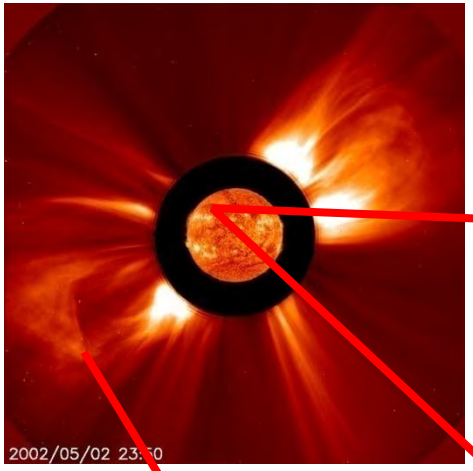
2011 DIB★CIP Meeting
25 August 2011

Space Weather Prediction Center

Our Mission: To provide space weather products and services that meet the evolving needs of the Nation.

Our Vision: A Nation prepared to mitigate the effects of space weather through the understanding and use of alerts, forecasts, and data products.

Three Varieties of Space Weather



93 Million Miles from Sun to Earth

Bursts of **Electromagnetic Radiation**

8 minutes

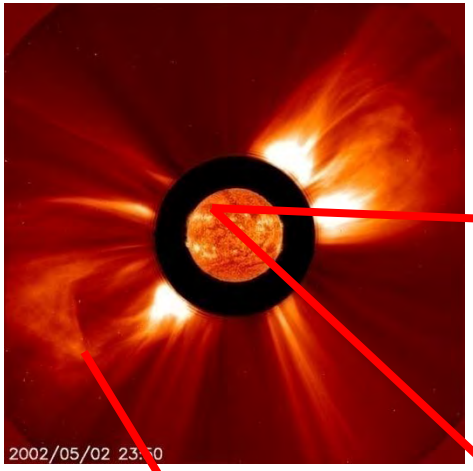
Showers of **High Energy Particles**

10-30 minutes

Tsunamis of **Magnetized Plasma**

18-96 hours

Three Varieties of Space Weather



93 Million Miles from Sun to Earth

Bursts of **Electromagnetic Radiation**

8 minutes

Disruption of GPS and HF Radio Comms

Showers of **High Energy Particles**

10-30 minutes

Satellite upsets and radiation threats to astronauts, air crews

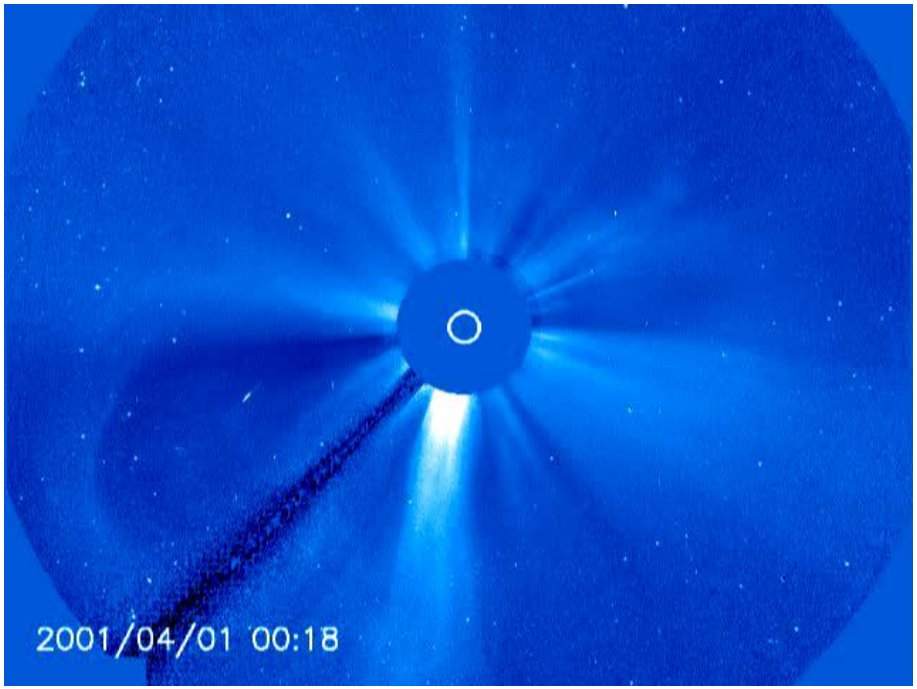
Tsunamis of **Magnetized Plasma**

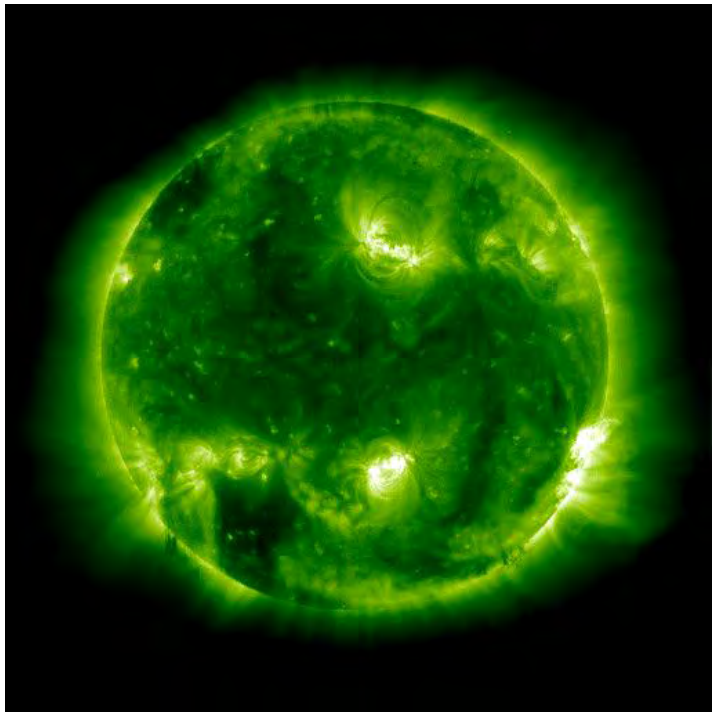
18-96 hours

Damage to power grids and disruption to polar HF Radio Comms

Two Types of Phenomena

"SOLAR TSUNAMIS"
CORONAL MASS EJECTIONS





"SOLAR TORNADOS"
SOLAR FLARES

High Energy Particles

Magnetized Plasma

Electromagnetic Radiation

Space Weather Impacts From Electromagnetic Radiation

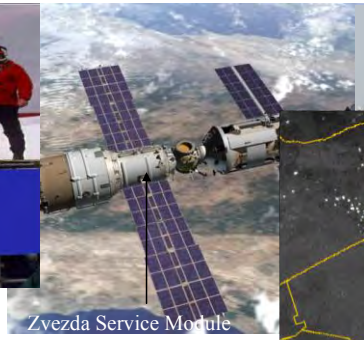
Electromagnetic Radiation

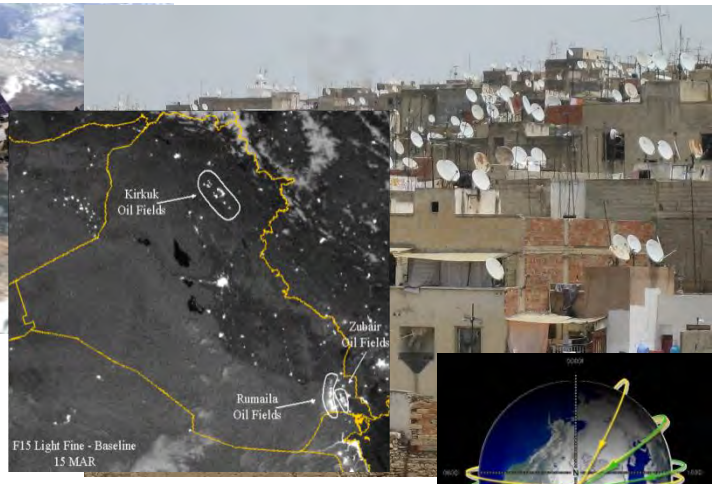
8 minutes

- Ionizes the upper atmosphere.
- Produces scintillation of radio signals and GPS.

"SOLAR TORNADOS"

Space Weather Impacts From High Energy Particles


Zvezda Service Module



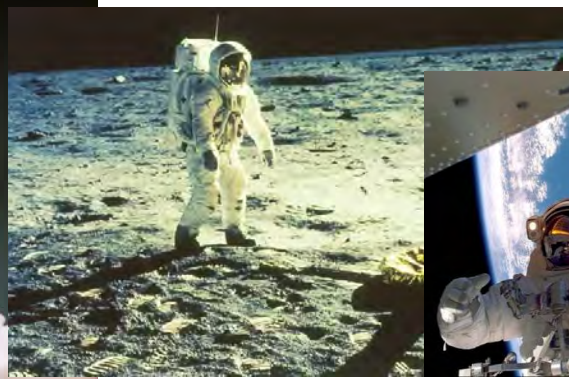
"SOLAR TSUNAMIS"

"SPACE TORNADOS"

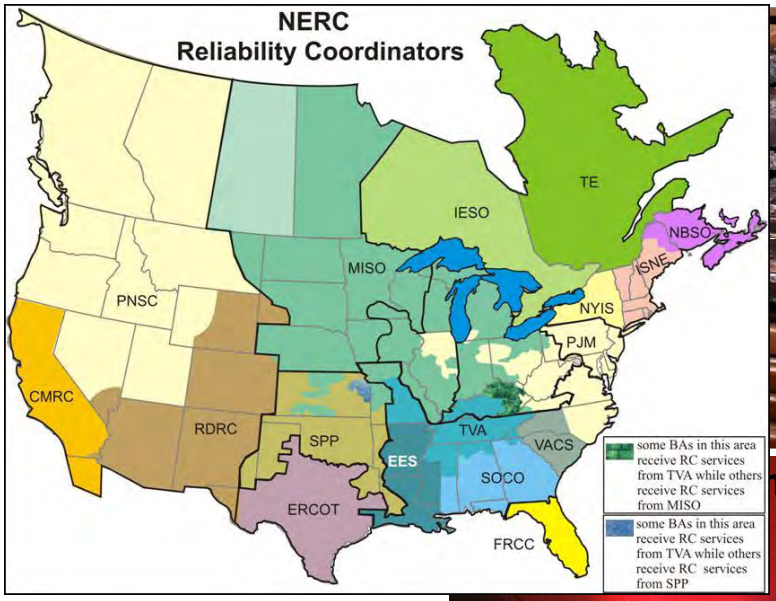
Damages sensitive electronics, creates electric discharges, sickens astronauts.

High Energy Particles

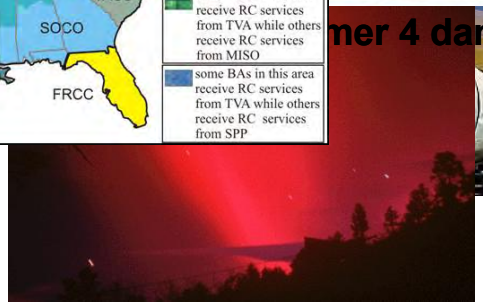
10-30 minutes



Space Weather Impacts From Magnetized Plasma



mer 4 damage



Generates Spurious Electric Currents.

"SOLAR TSUNAMIS"

Magnetized Plasma

18-96 hours

Our Nation's Evolving Needs

Working with White House, Congress, and government leadership.

Coordinating on ways forward to develop and implement mitigation strategies to safeguard critical infrastructure from the impacts of severe space weather.

- **Secure High-voltage Infrastructure for Electricity from Lethal Damage Act (SHIELD Act)** *(11 Feb, 2011)*
- **Meeting at White House with National Security Staff and OSTP** *(18 Feb, 2011)*
- **Op Ed on space weather by Holdren and Beddington** *(10 Mar,2011)*
- **Electric Infrastructure Security Summit (EISS) in Capitol building** *(11 Apr, 2011)*


The New York Times

The Opinion Pages

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH

I.H.T. OP-ED CONTRIBUTOR

Celestial Storm Warnings

By JOHN P. HOLDREN and JOHN BEDDINGTON
Published: March 10, 2011

Weather is often in the headlines. But largely unnoticed last month was the weather that forced airlines flying the polar route between the United States and Asia to detour south over Alaska. This unusual routing was a response to a "space weather" event — an enormous ejection of charged gas from the Sun capable of scrambling terrestrial electronic instruments.

***John P. Holdren** is the science and technology adviser to President Barack Obama. **John Beddington** is the chief scientific adviser to Prime Minister David Cameron.*


The New York Times

Opinion

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH

EDITORIALS COLUMNISTS CONTRIBUTORS LE

OP-ED CONTRIBUTOR

The Sun Also Surprises

By LAWRENCE E. JOSEPH
Published: August 15, 2010

Los Angeles

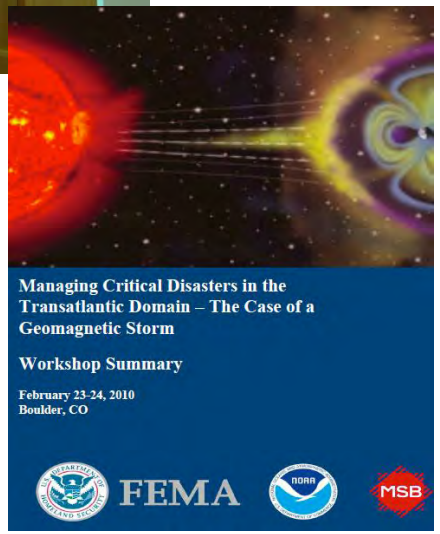
DESPITE warnings that New Orleans was unprepared for a severe hit by a hurricane, America was blindsided by Hurricane Katrina, a once-in-a-lifetime storm that mad years ago this month. W similarly unready for an potential natural disast storms, bursts of gas on surface that release tren energy pulses.

Safeguarding Our Nation's Advanced Technologies

Space Weather and Emergency Managers

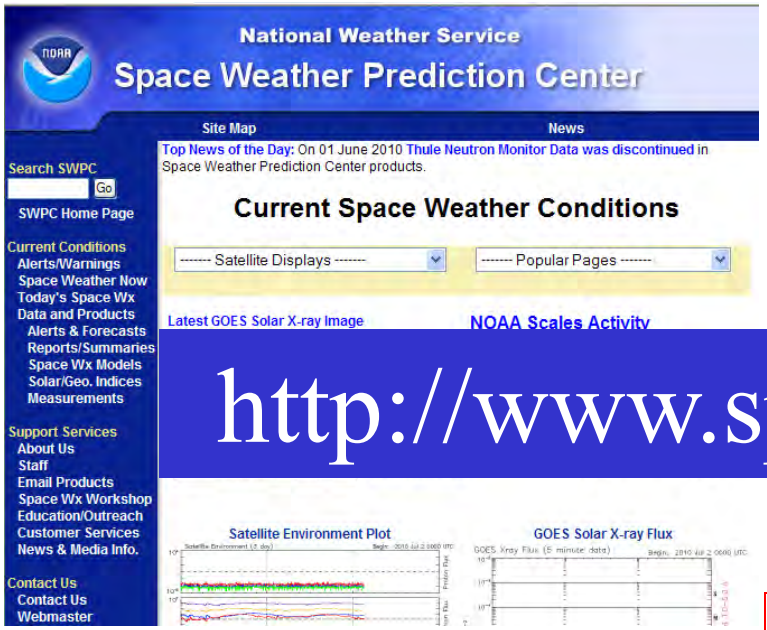
- FEMA Administrator Fugate visits SWPC
- FEMA Region VIII designated as Space Weather Center of Excellence for FEMA
- Workshop on managing space weather disasters in Transatlantic domain with EU/EC and Sweden held in Boulder (Feb 2010)
- SWPC brief FEMA Leadership at FEMA HQ and FEMA Regions
- Space weather warnings now distributed to FEMA National Response Coordination Center NRCC and FEMA Operations Center

FEMA



Safeguarding Our Nation's Advanced Technologies

NOAA Space Weather Scales



Radio Blackouts: R1-R5

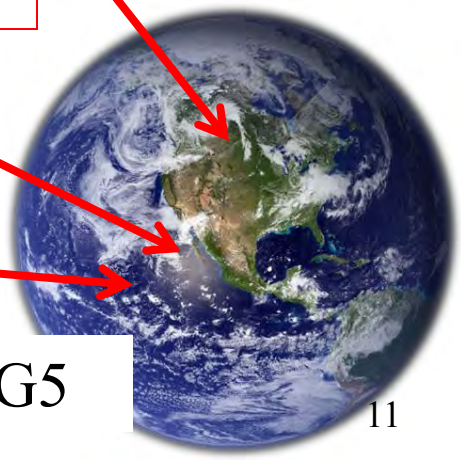
Electromagnetic Radiation

Category 5 Storms and Blackouts are High Impact/ Low Frequency Events

http://www.spaceweather.gov

Radiation Storms: S1-S5

High Energy Particles



Magnetized Plasma

Geomagnetic Storms: G1-G5

Combined Space Weather Services for the Nation

Observations Requirements

Space / Space Wx Operators

Environmental Inputs (DoD, Civil, International)

Data Received

AFWA – space weather data ingest/analysis/prediction and product flow to the warfighter

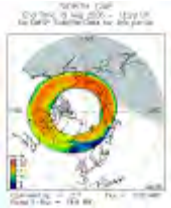
SWPC – space weather data ingest/analysis/prediction and product flow to the civil sector

Data & Products Provided

AFWA: Space Wx support provider

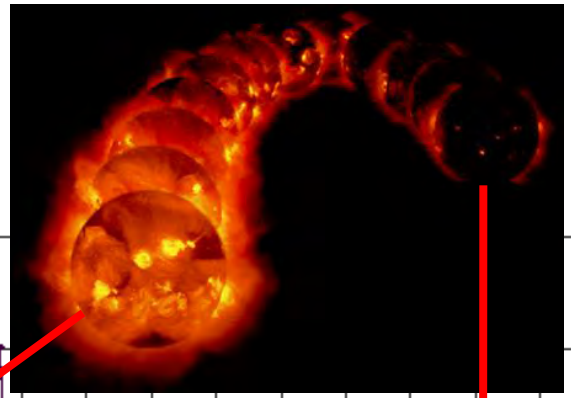
2 WS
Space Weather Flight

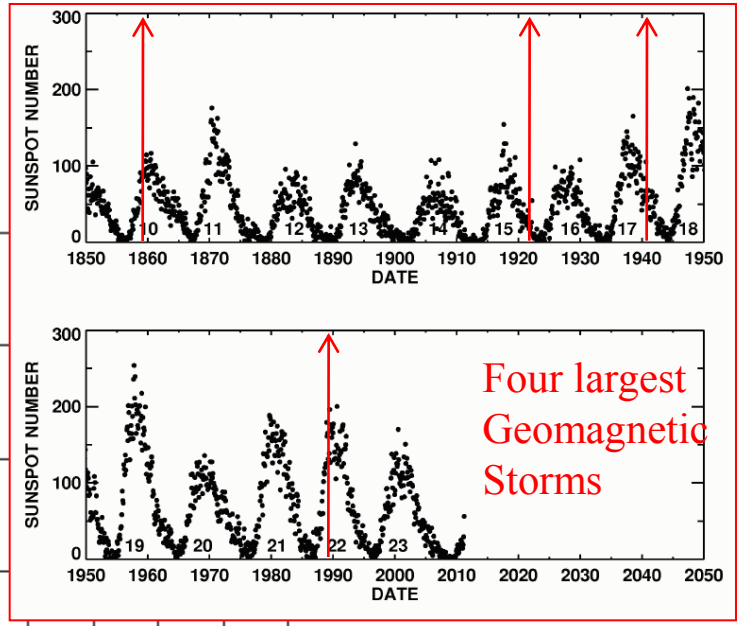
Teamwork



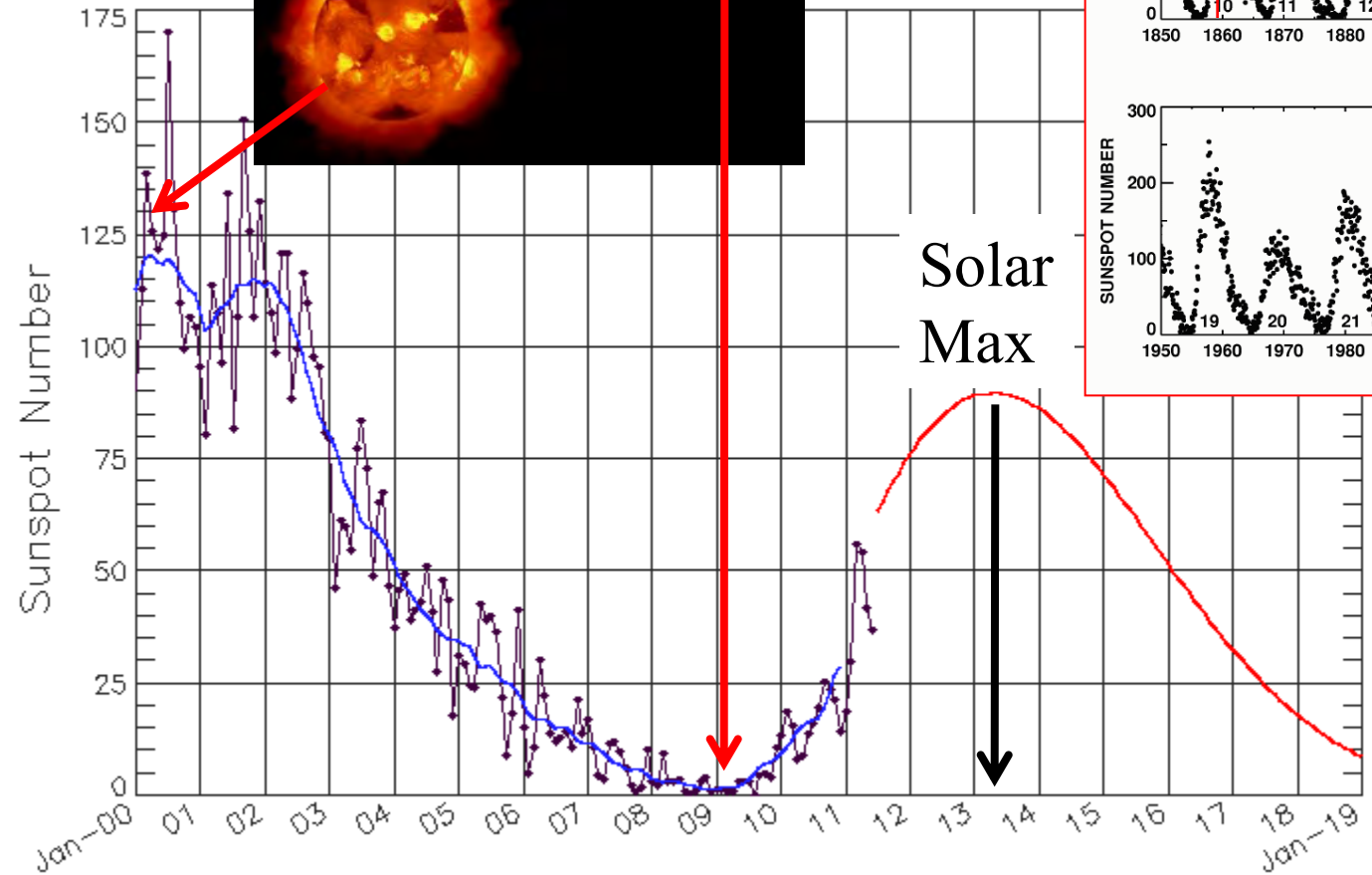
Tailored Products

More Space Weather Ahead…

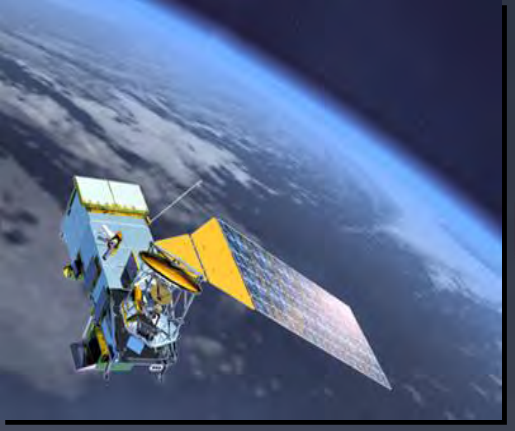


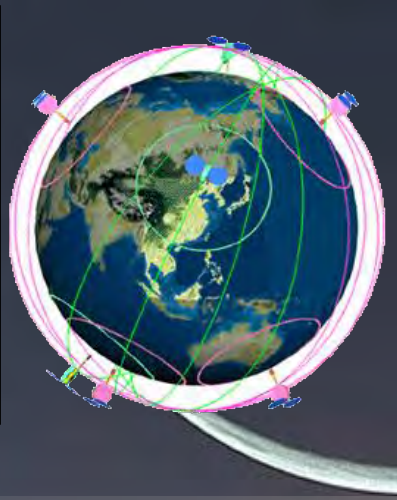


Solar Max



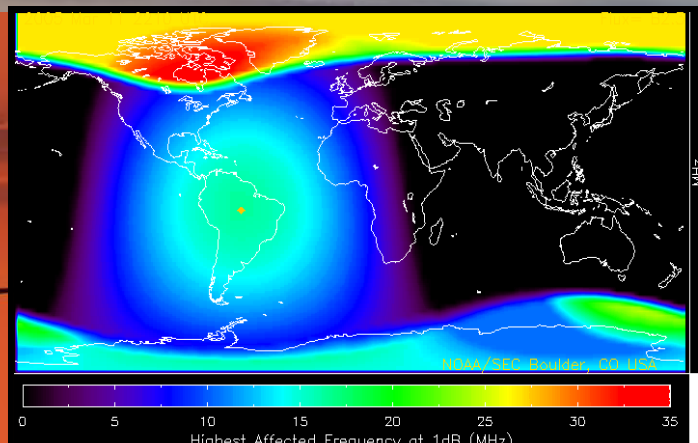
The Sun's Activity Cycle is about 11 years in length

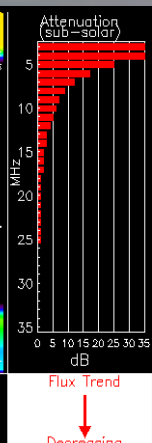




SWPC's Goal:

Provide the *right* information… in the *right* format...
at the *right* time… to the *right* people…
to make the *right* decisions





The Future of Response, Recovery and Reconstitution Capability

Sheraton Society Hill Hotel, Philadelphia, PA

William L. Carwile, III

Associate Administrator for Response and Recovery

August 25, 2011

FEMA

Presentation Overview

- ***Federal Authorities***
  - *Stafford Act of 1988 (42 USC 5121-5206)*
  - *Post Katrina Reform Emergency Management Act (PKREMA) of 2006 (P.L.109–295—OCT. 4, 2006)*
- ***National Response Framework (NRF)***
- ***FEMA Operations***
  - *National Response Coordination Center (NRCC), Regional Response Coordination Centers (RRCC), and Joint Field Offices (JFOs)*
- ***Whole Community***
  - *Whole Community Principles, Maximum of Maximums, and Core Capabilities*
- ***Building state and local capacity***
  - *Supporting state and local governments*

FEMA

Federal Authorities

- *Stafford Act of 1988*
  - Amended the Disaster Relief Act (DRA) of 1974. The Stafford Act constitutes the statutory authority for most Federal disaster response activities especially as they pertain to the Federal Emergency Management Agency (FEMA) and FEMA programs.
  - Provides legislative authority to assist governors, communities, and individuals.
- *The Post Katrina Emergency Management Reform Act (PKEMRA):*
  - Enhanced FEMA's responsibilities in leading and supporting the nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation.
  - The FEMA Administrator will serve as the principal advisor to the President, Homeland Security Council, and the Secretary for all matters relating to emergency management in the United States.

FEMA OPERATIONS

FEMA

Bill Carwile August 25, 2011

National Response Framework (NRF)

Core Document

The NRF provides doctrine, organization, roles and responsibilities, response actions and planning requirements that guide national response

Response Doctrine
- Engaged Partnership
- Tiered Response
- Scalable, flexible, and adaptable operational capabilities
- Unity of Effort-Unified Command
- Readiness to Act

NRF Resource Center

Emergency Support Function Annexes	**Mechanisms to group and provide Federal resources and capabilities to support State and local responders.**
Support Annexes	**Essential supporting aspects of Federal response common to all incidents.**
Incident Annexes	**Incident-specific applications of the Framework.**
Partner Guides	**Next level of detail in response actions tailored to the actionable entity.**

Coordination Centers

❑ *National Response Coordination Center (NRCC)*

- Operational element of DHS National Operations Center
- NRCC is a multi-agency center that provides overall Federal support coordination for major disasters and emergencies

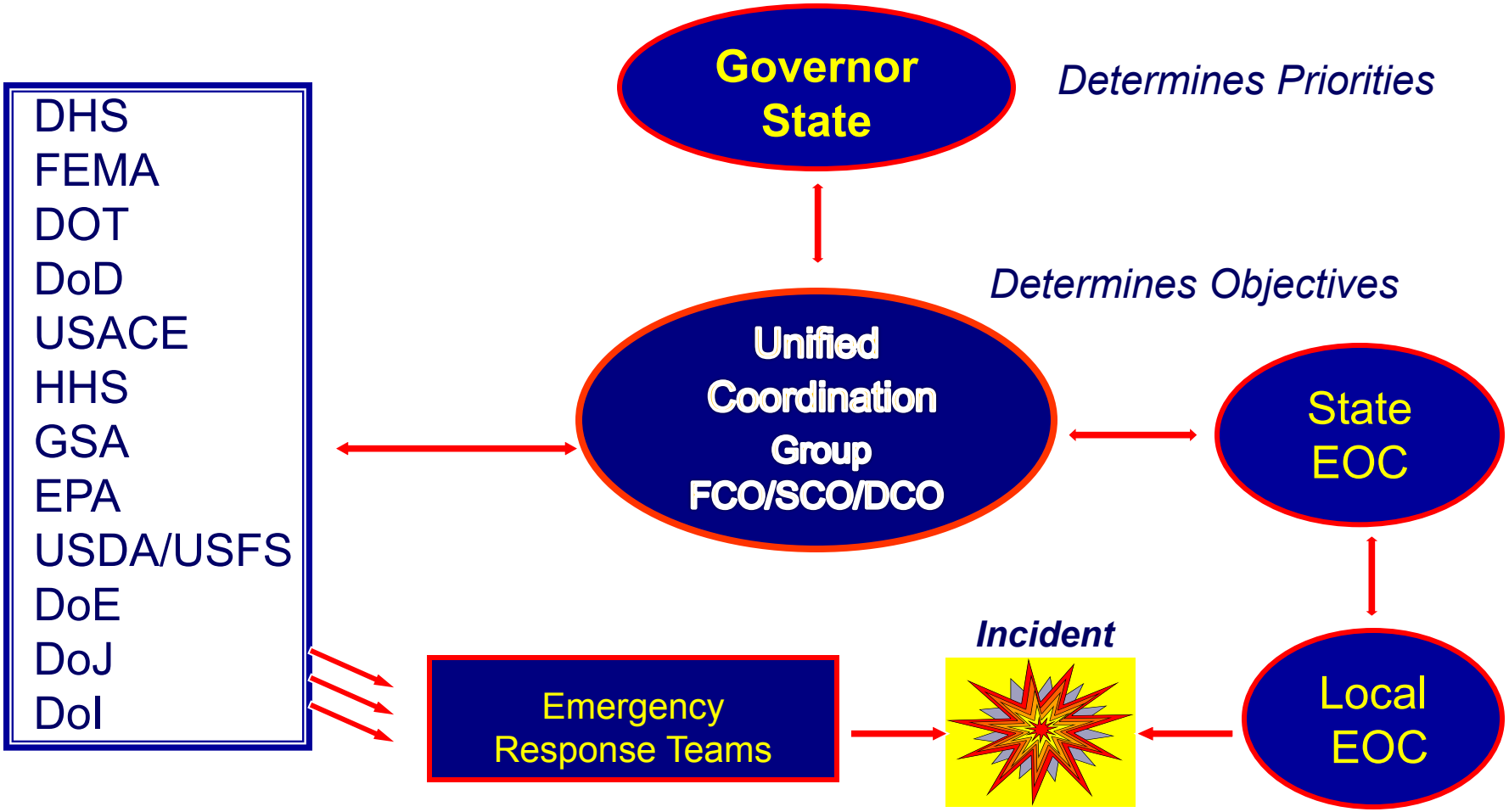
❑ *Regional Response Coordination Centers (RRCCs)*

- Regionally-based multi-agency coordination center team; Regional lead in coordinating disaster response operations.

❑ *National Watch Center (NWC)*

- Links RRCCs, regional DHS components, National and Regional Department and Agency leads for ESFs, NJTTFs, DOD Operations Centers, and other key Federal, state, and local operational centers
- Activates and deploys national level teams such as the Incident Management Assistance Team (IMAT), and Urban Search and Rescue Task Forces (US&R)

Joint Field Office (JFO) Relationships



******The JFO supports the needs of the State******

FEMA

Whole Community

FEMA

Bill Carwile August 25, 2011

Whole Community

- Calls for a holistic, rather than government-centric approach to emergency management.

- FEMA is but one part of the Nation's emergency management team– the Whole Community makes up the whole team.

- We can't plan for easy, we must plan for the real– for the actual communities we live in.
  - 57 million Americans with disabilities or approximately 20% of the US population.
  - Twenty-seven percent of the US population is under the age of 19.
  - Thirteen percent of the US population is over the age of 65.

- Whole Community is a more inclusive approach to emergency management that embraces all facets of society

FEMA

Meta-Scenario

- In order to anticipate catastrophic requirements and to avoid narrow focus on a limited number of specific scenarios, the Whole Community methodology is built upon a foundation of a meta-scenario consisting of the maximum of maximum challenges across a range of scenarios:
- No-notice event
- Impact area
  - ~7 million population
  - 25,000 square miles
  - Several states and FEMA regions
- 190,000 fatalities in initial hours
- 265,000 citizens require emergency medical attention
- Severe damage to critical infrastructure and key resources
- Severe damage to essential transportation infrastructure
- Ingress/egress options limited

FEMA

Core Capabilities

Represent the highest priority essential functions necessary for both saving and sustaining lives, and stabilizing the site and the situation within 72 hours.

Enables Response

- Situational Assessment
- Public Messaging
- Command, Control, & Coordination
- Critical Communications
- Environmental Health & Safety
- Critical Transportation

Survivor Needs

- On-Scene Security and Protection
- Mass Search and Rescue Operations
- Health and Medical Treatment
- Mass Care Services
- Public & Private Services & Resources
- Stabilize and Repair Essential Infrastructure
- Fatality Management Services

FEMA

Bill Carwile August 25, 2011

Building Capacity at State and Local Levels

- FEMA's Grant Program Directorate (GPD) is responsible for 18 preparedness grant programs and has awarded over $32B in grant money to all 50 states and 6 territories—including the District of Columbia—to bolster state and local jurisdictions preparedness, and response capabilities. Below are a few examples of how grant dollars have been expended over the years at the state and local levels:

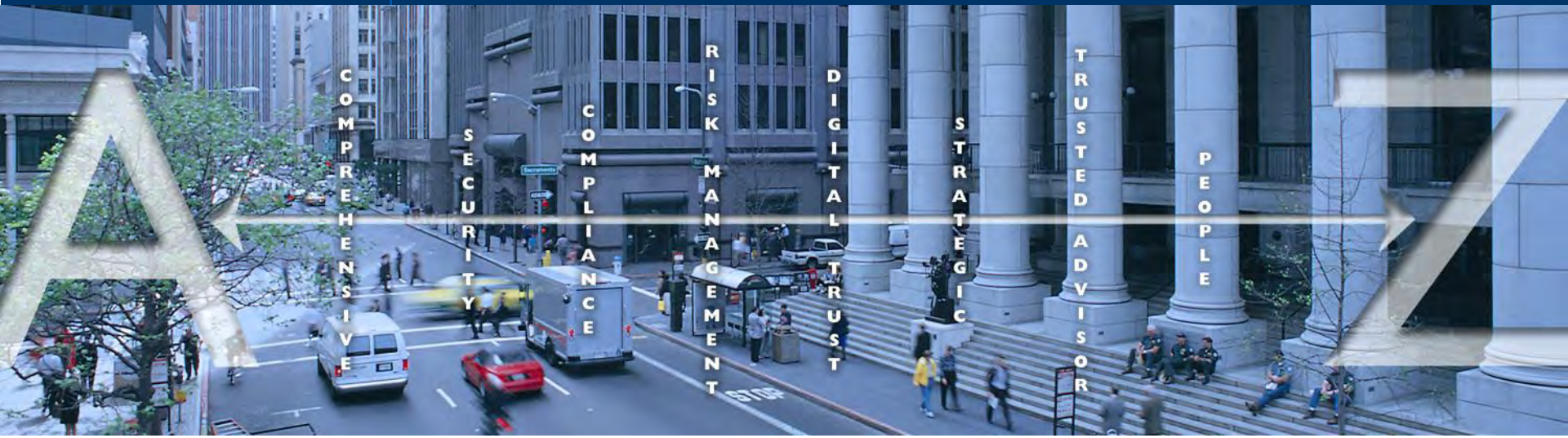
  - Building and sustaining community resilience;
  - Strengthening state and local security initiatives;
  - Improving critical communication networks and systems;
  - Training and preparing urban search and rescue teams, including K-9 units and;
  - Improving transit and building infrastructure

FEMA

FEMA

Infrastructure Dependencies: The Big Rocks Panel - Private Sector Perspective

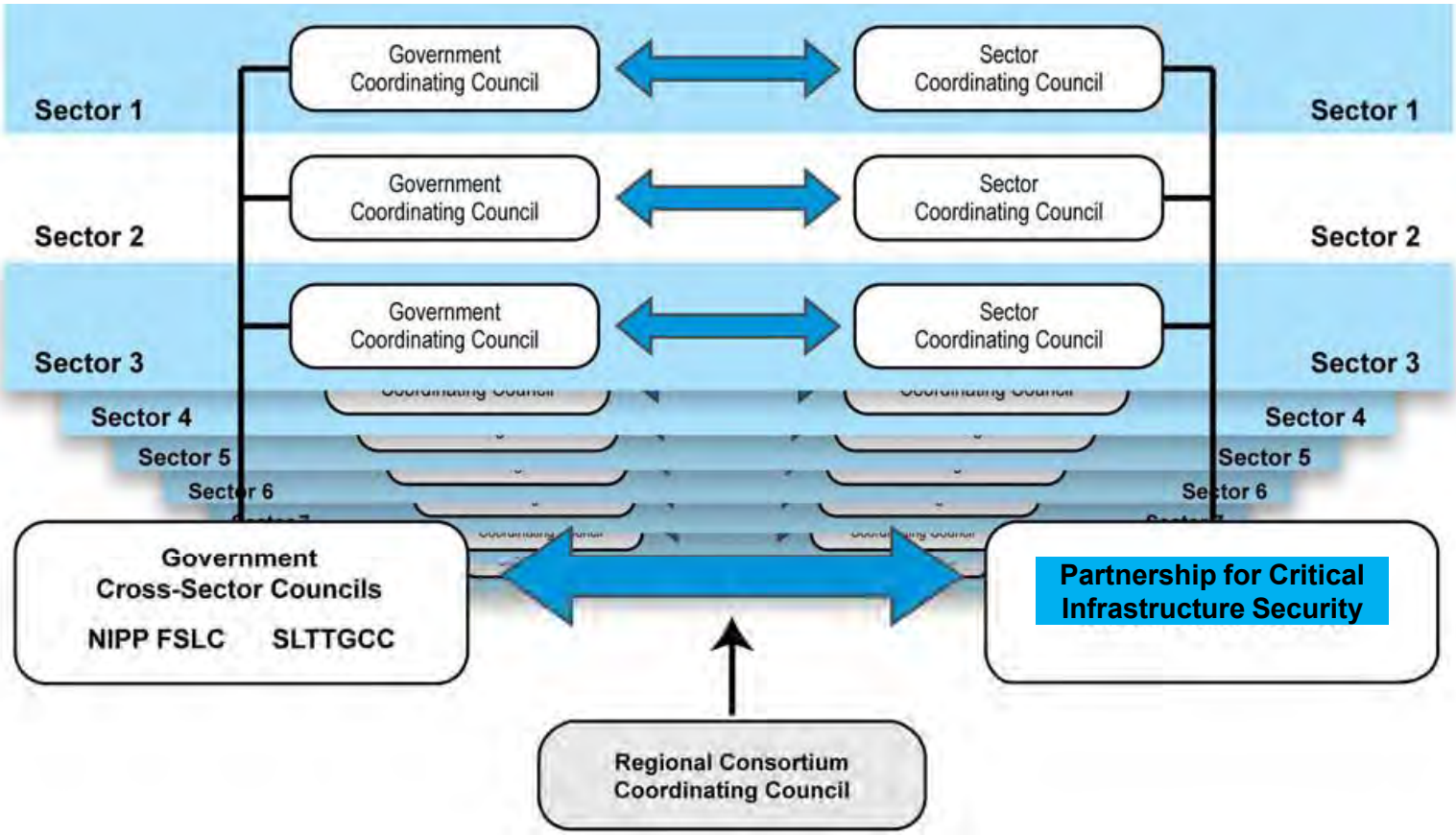
DIB CIP Conference, 24 August 2011



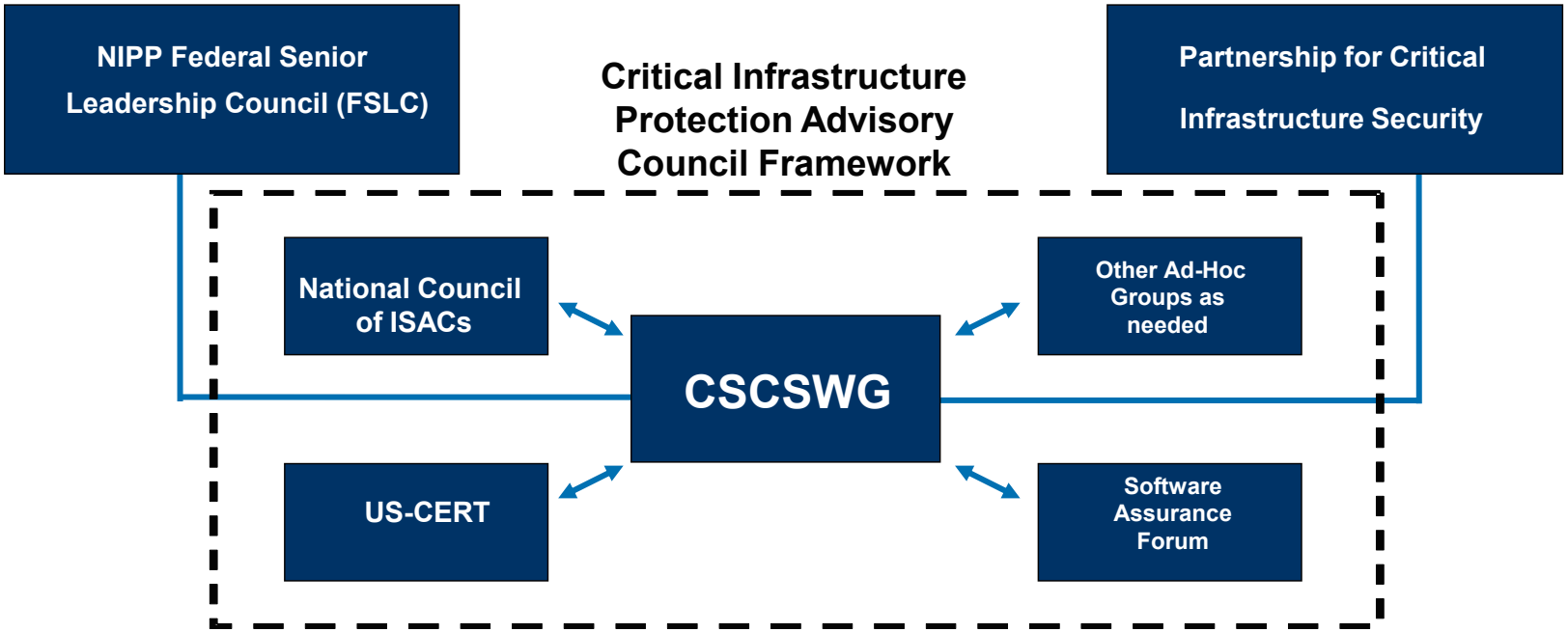
Guy Copeland, Vice President, Information Infrastructure Advisory Programs and Special Assistant to the CEO, CSC
Co-Chair, Cross Sector Cyber Security Working Group (CSCSWG)

CSC

Sector Partnership Model
National Infrastructure Protection Plan (NIPP)
Critical Infrastructure Partnership Advisory Council (CIPAC)



Cross-Sector Cyber Security Working Group
CIPAC Framework and Liaison Groups



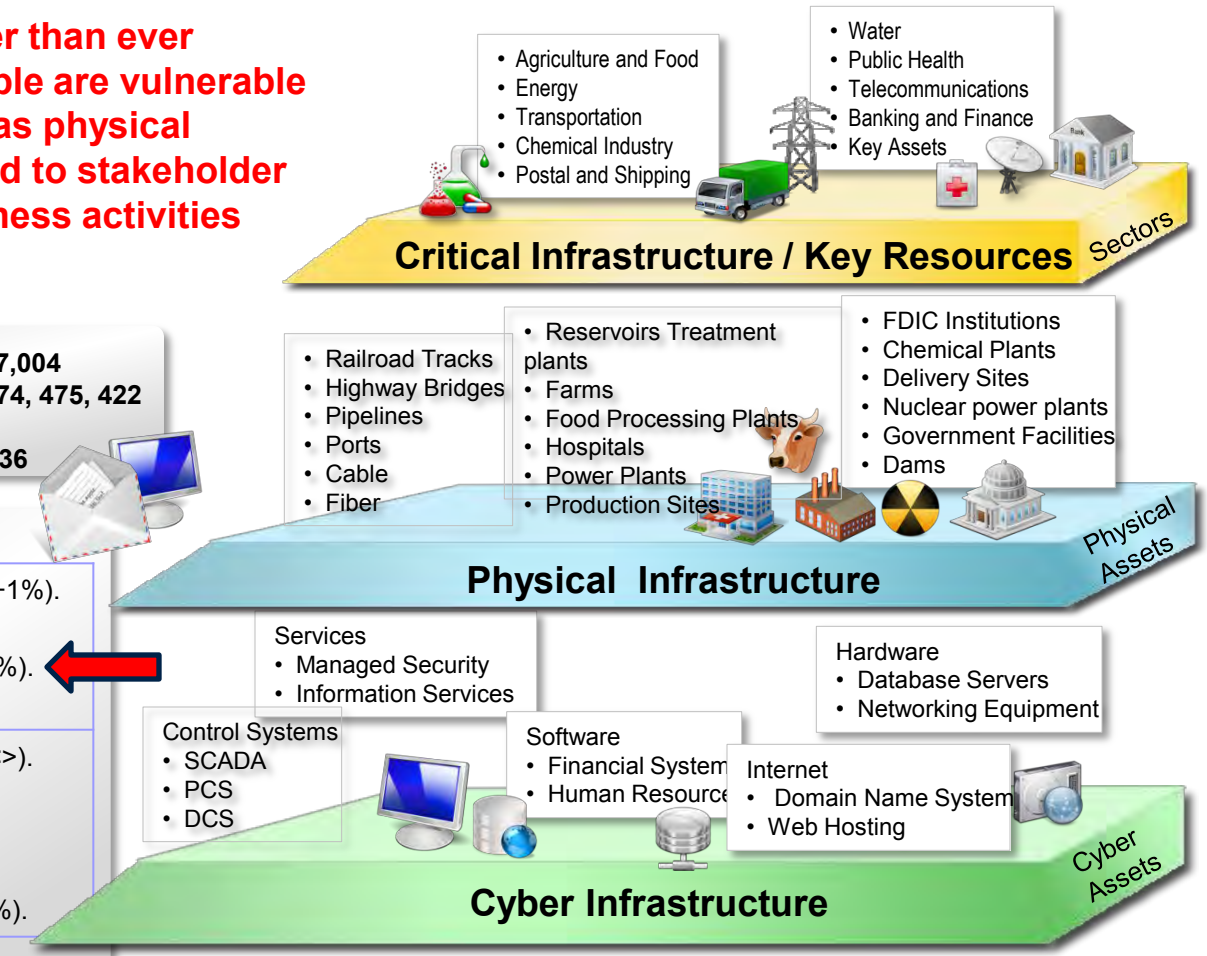
Dependencies on technology are greater then ever

- Possibility of disruption is greater than ever because hardware/software/people are vulnerable
- Economic disruption as serious as physical
- Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities

Internet users in the world: 1,766,727,004
E-mail messages sent today: 215, 674, 475, 422
Blog Posts Today: 458, 972
Google searches Today: 2,302,204,936

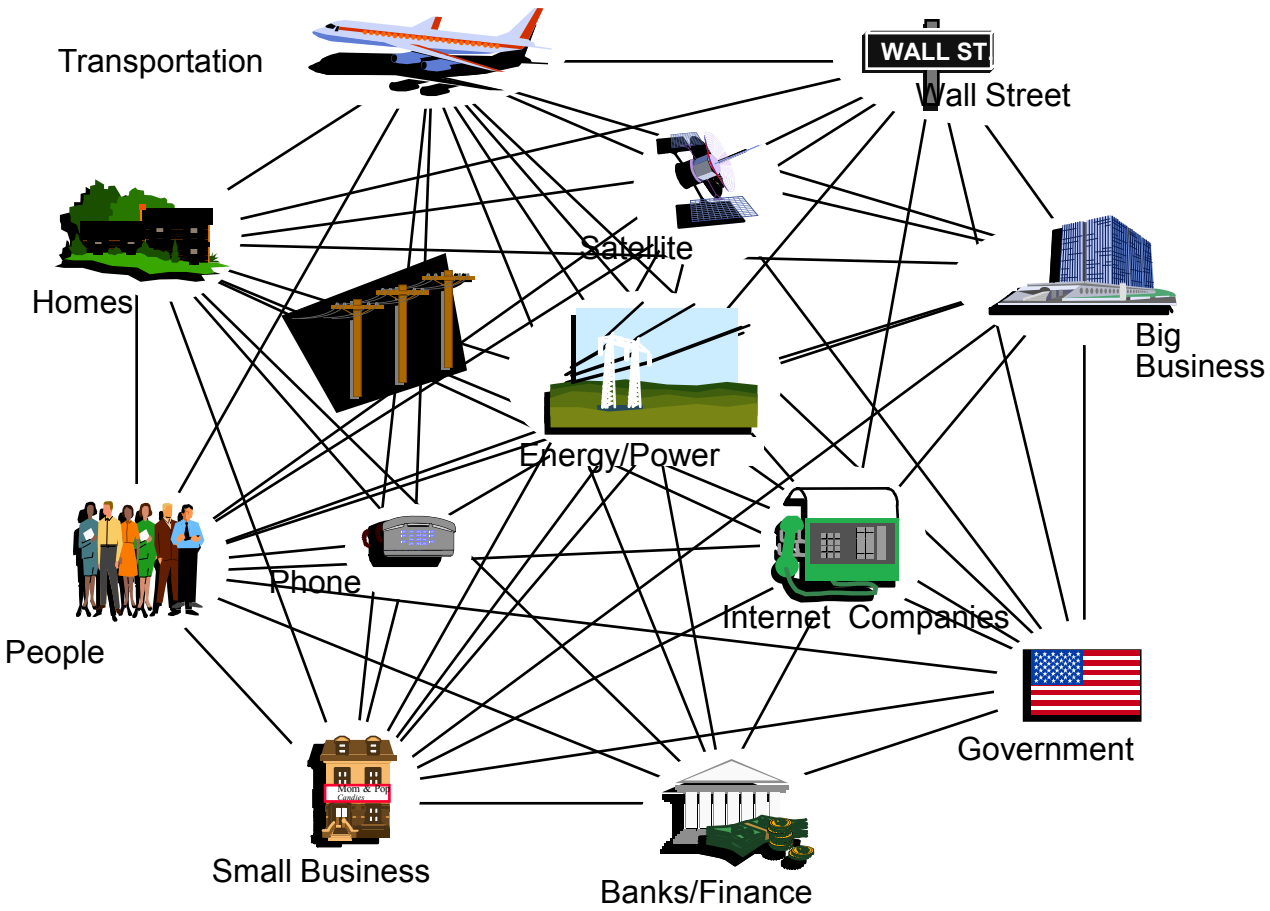
Who is behind data breaches?	**74%** resulted from external sources (+1%). **20%** were caused by insiders (+2%). **32%** implicated business partners (-7%). **39%** involved multiple parties (+9%).
How do breaches occur?	**7%** were aided by significant errors (<>). **64%** resulted from hacking (+5%). **38%** utilized malware (+7%. **22%** involved privilege misuse (+7%). **9%** occurred via physical attacks (+7%).

** Source – 2009 Verizon Data Breach Investigations Report*



credit to Don Davidson, DoD

Private Sector Impact:
Interdependencies among infrastructures make a problem in one infrastructure a problem for all.



Conclusions – We Have Known For Years Now

- National risk is growing, especially with asymmetric threats and increasing reliance on information & communications infrastructure
- Public confidence in infrastructures is critical
- Risk is shared among public & private interests
- New Thinking Required

Partnership is the Foundation for Critical Infrastructure Security

Partnership Principles

- Partnership must be voluntary
- Trust among partners is essential
- Working members must be personally responsible and accountable for their trusted behavior
- Objectives must be clearly defined and embody common goals
- Internal support and trust within each partner must exist
- Institutionalized process is important to provide lasting benefit
- Build on existing organizations first
- Working members of the partnership should frequently interact
- Partnership needs to be an evolving relationship
- Legal and liability issues can be powerful tools for aligning interests of the partners
- Partnership needs champions and institutional support

Successes and Challenges – a few examples

- National Infrastructure Protection Plan
  - Sectors, Sector Specific Plans and Risk Assessments
- National Level Exercises and Cyber Storm Exercises – joint
- Sharing through PCIS, National Council of ISACs, CSCSWG
- Private Sector Seats in NCCIC
- Cybersecurity is a Policy Concern and Priority
  - U.S. Senate: Lieberman-Collins, Rockefeller-Snow, Reid
  - Administration Legislation Proposal
  - International Strategy for Cyberspace
- Rapid Adoption of Cloud Computing
  - See http://assets1.csc.com/lef/downloads/Digital_Trust_in_the_Cloud.pdf
- National Broadband Plan and Public Safety
- Supply Chain and other international issues
- Telecom Energy Alliance Working Group

There are numerous successes and there remain numerous challenges!

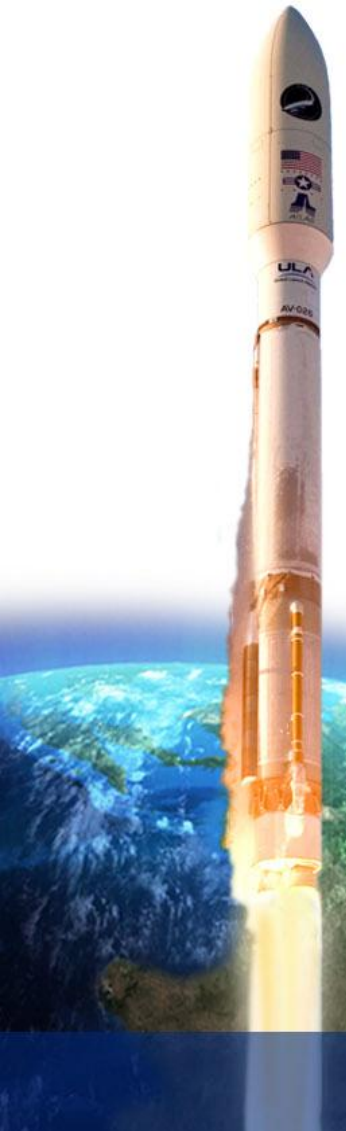
Guy Copeland, CSC

703-876-1238, gcopelan@csc.com

See http://www.csc.com/security/ and

http://www.csc.com/communications_media_and_entertainment/

United Launch Alliance



Engagement in Preparedness Panel

Philadelphia, PA

August 25, 2011

Overview of ULA

- Officially Formed December 2006 with the Combination of Two World Class Launch Systems: Boeing's Delta & Lockheed Martin's Atlas Expendable Launch Vehicle Businesses
- Single Provider of Launch Services to U.S. Government Customers
- Includes Evolved Expendable Launch Vehicles
- 3,800 Employees
- ULA's locations had solid Crisis Management Plans
  - Each were written specific to their site and heritage organization

United Launch Alliance

ULA Crisis Management Overview

ULA Crisis Management Overview

Starting Out

- Seven months after ULA's formation, natural disaster severely impacted one of our facilities.
  - Full loss of power from local services
  - 75% of facility was flooded
  - Disaster recovery firm required
  - Long-tail to recovery
  - While repair to infrastructure was required, no inventory loss and production was virtually uninterrupted.

- <u>Response</u>
  - Crisis Management Plan was state of the art for preparedness
  - Communication plans must be readily available, robust, tested and followed
  - Enterprise must be integrated and understand their roles
  - Disaster recovery firm engagement critical
  - Firm must be scalable and able to respond to the unique needs of the business
  - You may need to involve the local government into your planning to mitigate future damage

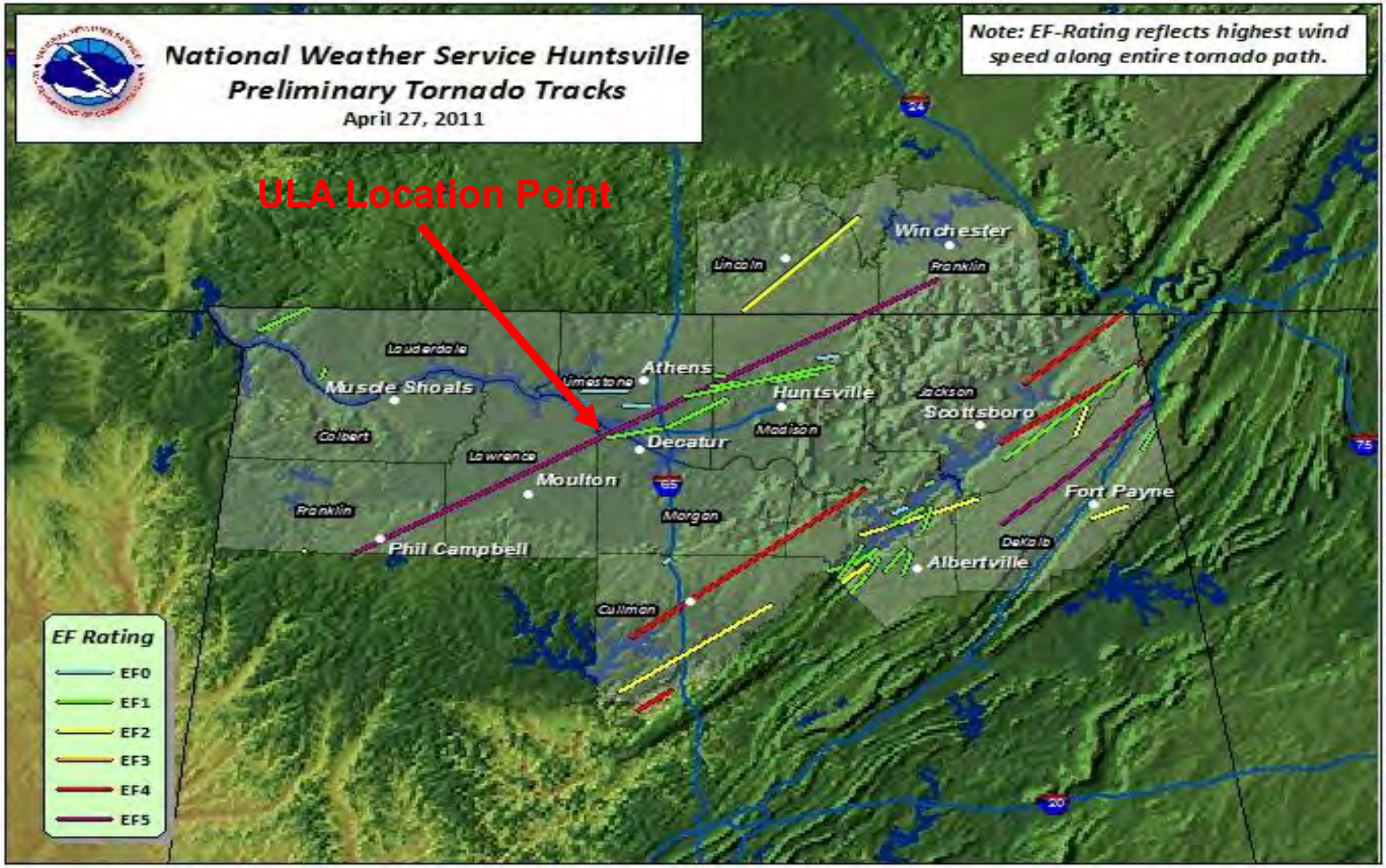
ULA Crisis Management Overview

2011 Alabama Tornado Disaster

- Tornado registered as EF-5
  - Conditions:
    - Winds estimated at 105 mph to 200 mph
    - Minor water intrusion
- Times of events: 0520 – 1600
  - 5 Evacuations
  - Delta Mariner notified via phone of weather conditions
  - 1530 Complete power lost to factory
  - 1600 Plant closed
  - 1630 All employees off site
- 1720 Emergency Operations Center Activated
  - Site lead, S&ES and plant operations
  - Monitored local conditions
  - Risk Management Notified - Disaster recovery firm activated
  - Executives notified

ULA Crisis Management Overview

2011 Tornado Tracks



ULA Crisis Management Overview

2011 Disaster Response

- 4-28-11 EOC fully staffed
- Disaster recovery firm on site
- ULA employees and onsite customers being accounted for
- Hardware and structure evaluation conducted
- Return to work preparation and communication being developed

Lessons Learned:

- Include engineering and production lead into EOC
- Improve communication with employees
- Improve fueling process for site
  - Fuel diesel and gas units onsite
- Improve IT support
- Implement contracts with suppliers

IMPLEMENT LESSONS LEARNED IN BUSINESS CONTINUITY PROGRAM

United Launch Alliance

ULA's Business Continuity Program

Maturity Model Engagement in Preparedness

ULA's Business Continuity Program
Maturity Model Engagement in Preparedness

- Business Continuity Program Today:
  - Executive sponsored
  - Active steering committee
  - Business impact analysis nearly complete
    - Learning and active responses during the mapping

  Includes:
  - Crisis Management Program
    - Consistent plans readily available throughout organization
    - EOCs at sites understood
    - Regular exercises with Enterprise team
  - Information Technology Disaster Recovery Planning
  - Pandemic planning
  - Disaster recovery firm formally engaged

ULA's Business Continuity Program
Maturity Model Engagement in Preparedness

- Challenges and Lessons Learned on Business Continuity Planning
  - Get executive support
  - Active steering committee
  - Define required resources
  - Implement planning that fits the business
  - Awareness and training essential
  - BCP is NOT a project but a program
  - Ownership and accountability at the process level crucial
  - Understand your supply chain
  - Metrics matter
- Tips to Our Success:
  - Loss Control Program can be your partner
  - Don't delay action
    - Engagement of day-to-day learning and improvement necessary
  - Partner with disaster recovery firm capable of meeting your business needs
  - Test. Test. Test.
  - Communicate

The Office of Infrastructure Protection

National Protection and Programs Directorate

Department of Homeland Security

Protective Security Coordination Division Overview Brief

August 25, 2011

Homeland Security

The Role of Homeland Security

- Unify a national effort to secure America
- Prevent and deter terrorist attacks
- Protect against and respond to threats and hazards to the Nation
- Respond to and recover from acts of terrorism, natural disasters, or other emergencies
- Coordinate the protection of our Nation's critical infrastructure across all sectors

Homeland Security

IP Vision and Mission

- Vision - A safe, secure, and resilient critical infrastructure based on and sustained through strong public and private partnerships

- Mission - Lead the national effort to mitigate terrorism risk to, strengthen the protection of, and enhance the all hazard resilience of the Nation's critical infrastructure

Homeland Security

The Threat

We will “hit hard the American economy at its heart and its core.”

- Osama bin Laden

Homeland Security

Threats May Come from All Hazards

Homeland Security

Critical Infrastructure Defined

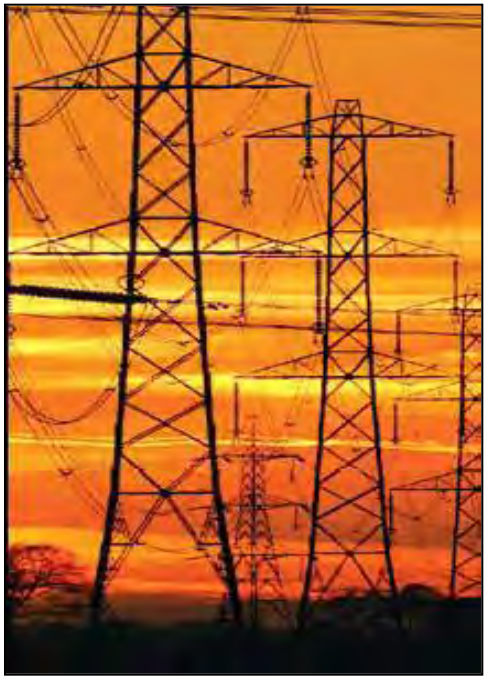
- Critical Infrastructure
  - "Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction."

Source: National Infrastructure Protection Plan (NIPP) 2009

Homeland Security

Critical Infrastructure Sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Commercial Nuclear Reactors, Materials, and Waste
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Drinking Water and Wastewater Treatment Systems
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation Systems



Homeland Security

Critical Infrastructure Protection Challenges

- Majority of critical infrastructure assets are privately-owned
  - DHS has limited legal authority to regulate security practices of private industry (exceptions: high-risk chemical facilities, Transportation Security Administration, United States Coast Guard)
- DHS works with industry and Federal, State, local, tribal, and territorial governments to protect critical infrastructure
  - Coordinated through the NIPP
- To help communities better protect the Nation's assets, DHS deployed Protective Security Advisors (PSAs) throughout the country

Protective Security Advisors (PSAs)

- 93 PSAs and Regional Directors, including 87 field deployed personnel, serve as critical infrastructure security specialists
- Deployed to 74 Districts in 50 States and Puerto Rico
- State, local, tribal, and territorial link to DHS infrastructure protection resources
  - Coordinate vulnerability assessments, IP products and services, and training
  - Support response, recovery, and reconstitution efforts of States affected by a disaster
  - Provide vital link for information sharing
  - Assist facility owners and operators with obtaining security clearances
- During contingency events, PSAs support the response, recovery, and reconstitution efforts of the State(s) by serving as pre-designated Infrastructure Liaisons (IL) and Deputy ILs at the Joint Field Offices (JFO)
- Developed over 125,000 individual working relationships with Federal, State, local, tribal and territorial critical infrastructure protection partners

Protective Security Coordination Division (PSCD) Risk Mitigation Training

- Provide protection personnel in public and private sectors with specialized security training to prevent and protect against continuing and emerging threats to our Nation's infrastructure

- Examples of courses include:
  - Surveillance Detection Course
  - Soft Target Awareness Course
  - Protective Measures Course
  - Private Sector Counter-Terrorism Awareness Workshop
  - Improvised Explosive Device Awareness Workshop
  - Bomb-Making Materials Awareness Program

Homeland Security

Risk Mitigation Training

- Surveillance Detection Course
  - Provides a guideline for mitigating risks to critical infrastructure through developing, applying, and employing protective measures and the creation of a surveillance detection plan
- Protective Measures
  - Provides the knowledge and skills to understand common vulnerabilities and employ effective protective measures to enhance commercial sector awareness on how to devalue, detect, deter, and defend facilities from terrorism
- Private Sector Counterterrorism Awareness Workshop
  - Provides private sector security professionals with current strategies on soft target awareness, surveillance detection, and IED recognition, and outlines specific counterterrorism awareness and prevention actions that reduce vulnerability and mitigate the risk of domestic terrorist attacks
- Soft Target Awareness Course
  - Provides private sector security and safety personnel terrorism awareness, prevention, and protection information
- IED Awareness Workshop
  - Provides a basic awareness of IED prevention measures and planning protocols and the current technology and trends that characterize IEDs

Protected Critical Infrastructure Information (PCII) Program

- The PCII Program is an important tool to encourage industry to share their sensitive critical infrastructure information
- Established under the Critical Infrastructure Information Act of 2002, the PCII Program protects voluntarily submitted critical infrastructure information from:
  - Freedom of Information Act (FOIA)
  - State and local sunshine laws
  - Civil litigation proceedings
  - Regulatory usage
- Provides private sector with legal protections and “peace of mind”
- To qualify for PCII protections:
  - Information must be voluntarily submitted and not customarily in the public domain
  - Information cannot be submitted in lieu of compliance with any regulatory requirement

Homeland Security

Infrastructure Protection Report Series

- Increase awareness and improve understanding of infrastructure protection

Characteristics and Common Vulnerabilities

- Common Characteristics
- Consequences of Events
- Common Vulnerabilities

Potential Indicators of Terrorist Activity

- Surveillance Indicators
- Surveillance Objectives
- Transactional and Behavioral Indicators

Protective Measures

- General Protective Measures Options
- Specific Protective Measures Options per HSAS Level

- DHS has produced reports for 142 different asset types, including: Casinos, convention centers, hotels, education facilities, office buildings, shopping malls, stadiums, theme parks, residential buildings, and other commercial sector assets

Homeland Security

How Can You Help?

- Engage with your PSAs to facilitate protective actions and establish priorities and the need for information
- Assist in efforts to identify, assess, and secure critical infrastructures in your community
- Communicate local critical infrastructure protection related concerns
  - Business and economic ramifications of actions
  - Issues unique to the community

Homeland Security

Homeland Security

For more information visit:
www.dhs.gov/criticalinfrastructure

John Guest
Mid-Atlantic Regional Director
John.Guest@hq.dhs.gov

Accelerating Implementation of the Information Sharing Environment:
Building Beyond the Foundation

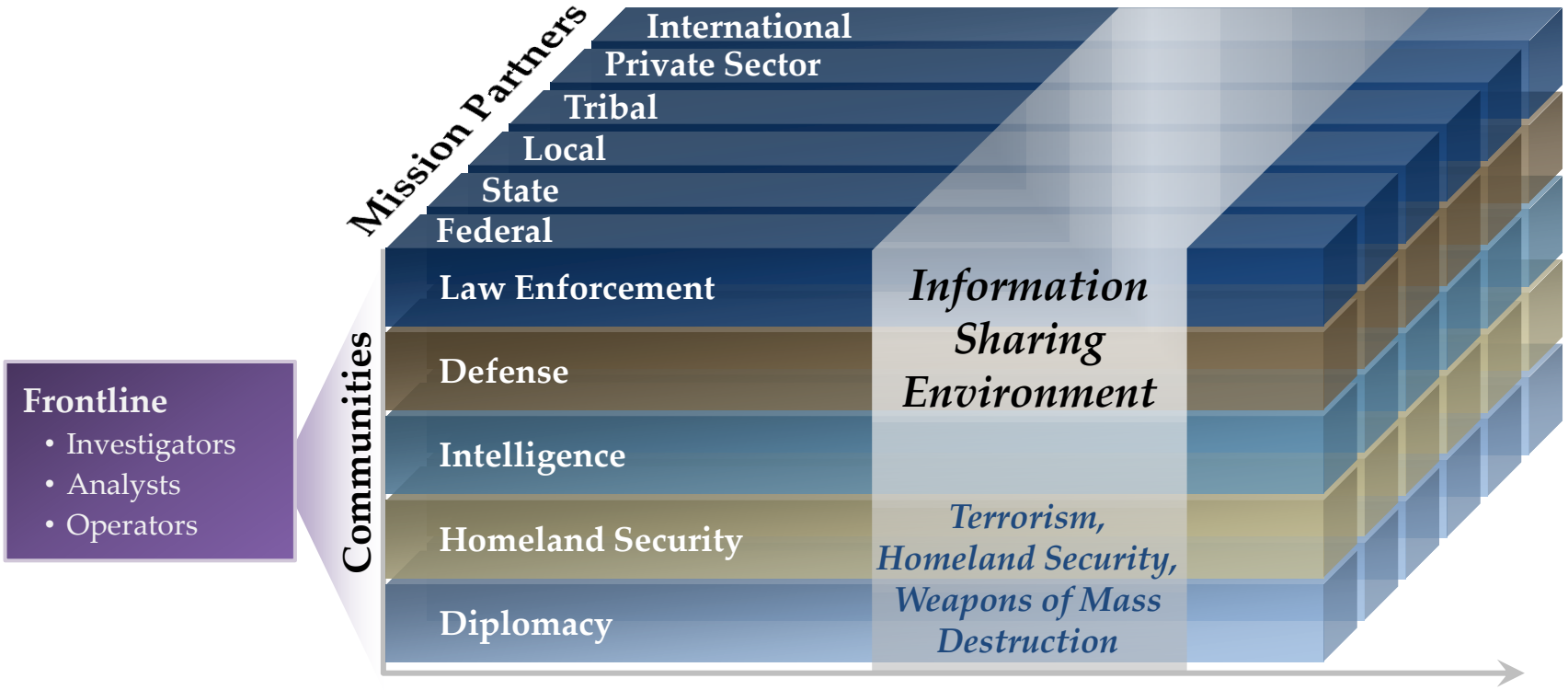
Michael Howell
Deputy Program Manager
Information Sharing Environment

25 August 2011
www.ise.gov

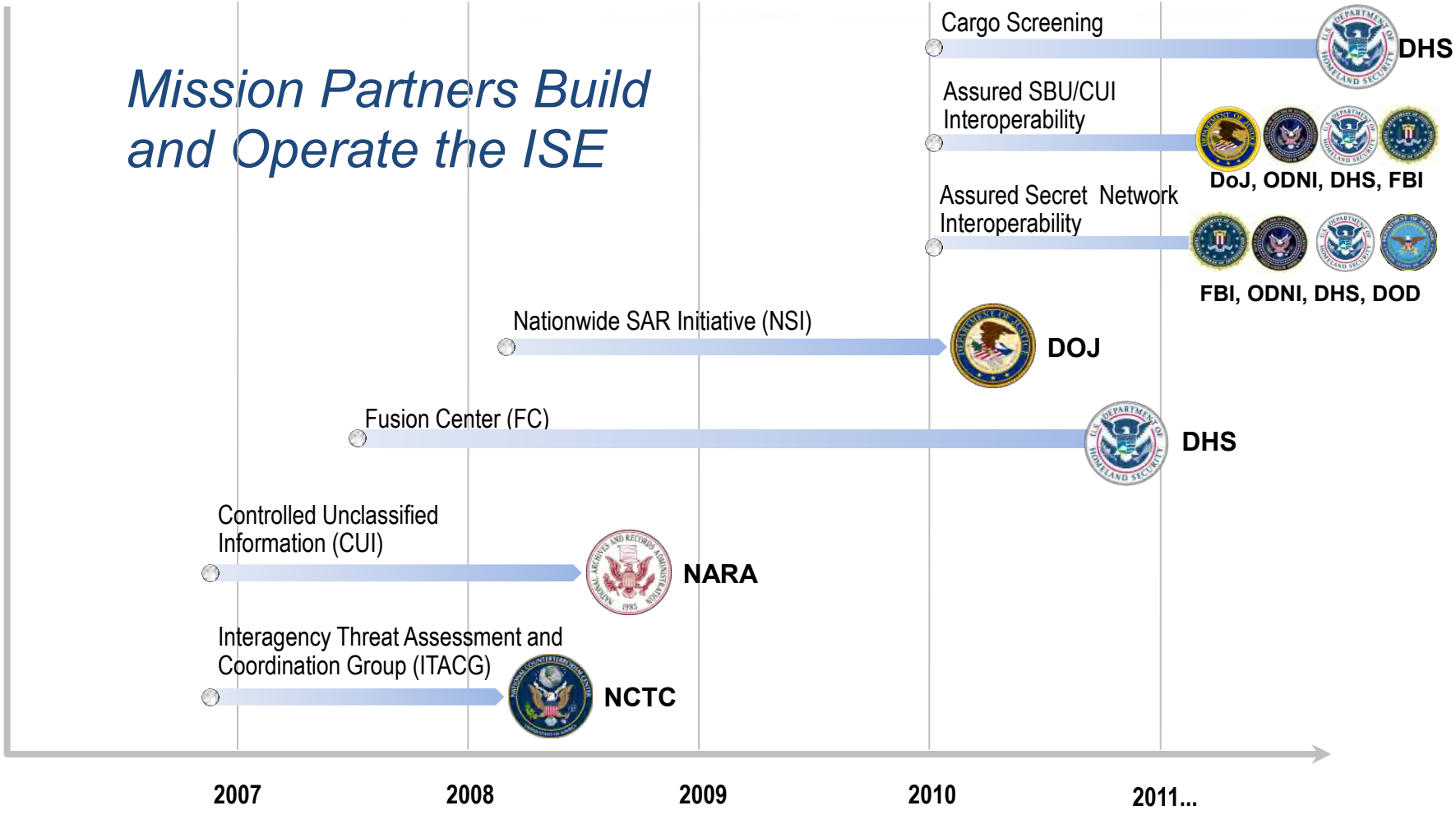
What is the Information Sharing Environment (ISE)?

- **Established:**
  - Post-9/11 Commission Reforms w/ the Intelligence Reform and Terrorism Prevention Act of 2004
- **Purpose:**
  - Align and leverage policies, processes, technologies, and systems
  - Promote timely, actionable, relevant information sharing re: counter-terrorism, WMD, and homeland security
  - Protect information, privacy, and civil liberties

Stakeholders & Mission



Business Model

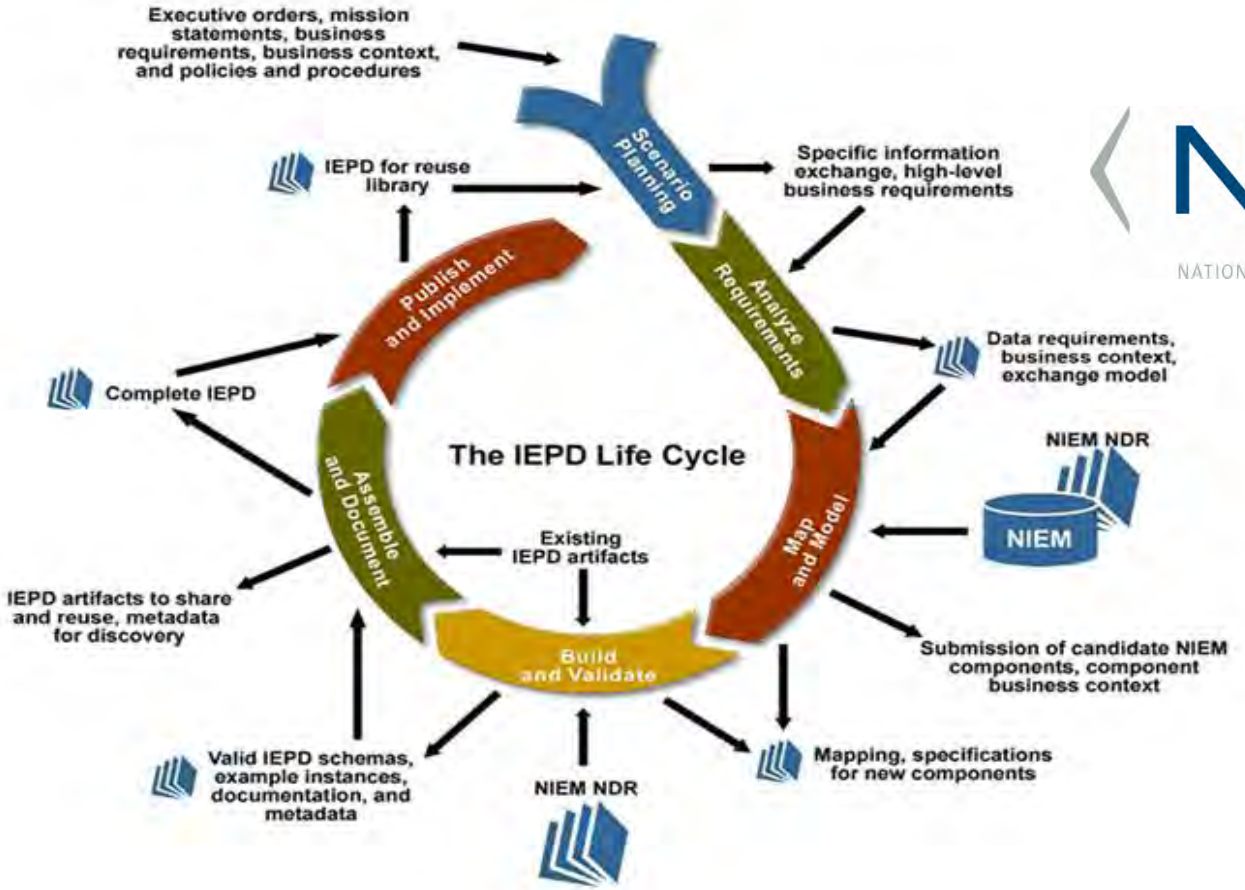


Priority Activities

- Strengthen Governance, Policy, Strategy and Coordination of Oversight
- Tag People. Tag Information. Manage Electronic Access to Classified Information
- Proactively Oversee the Management and Monitoring of Our Classified Networks and Information
- Strengthen Responsible Whole of Government Information Sharing and Safeguarding
- Leverage Standards to Lower Costs and Improve Performance

Example: Economical and Effective Information Sharing

Functional Standards:
National Information Exchange Model



NIEM
NATIONAL INFORMATION EXCHANGE MODEL

Example: Nationwide Suspicious Activity Reporting Initiative (NSI)

- The ISE in practice:
  - Uses a unified, **standards-based approach** to information sharing, while rigorously protecting the **privacy, civil rights, and civil liberties** of all Americans
  - **Integrates** state, local, and tribal law enforcement agencies' SAR processes into a nationwide effort
  - Leverages **existing processes** and systems

- The project is based on **standards** and **partnerships**

The Program Management Office is housed at DOJ BJA with strong partnerships with DHS and FBI.

Three Critical Issues

- Overcoming Organizational Resistance to Sharing
- Strengthening Information Sharing and Protection Together
- Adapting to Rapid and Accelerating Changes in Technology

Get Involved

Sign Up for Alerts and Join the Dialogue

- Events
- News
- Blogs
- Resources
- Communities

www.ISE.gov

Information Sharing: The Past, Present and Our Future

Chandra McMahon
Lockheed Martin
Chief Information Security Officer

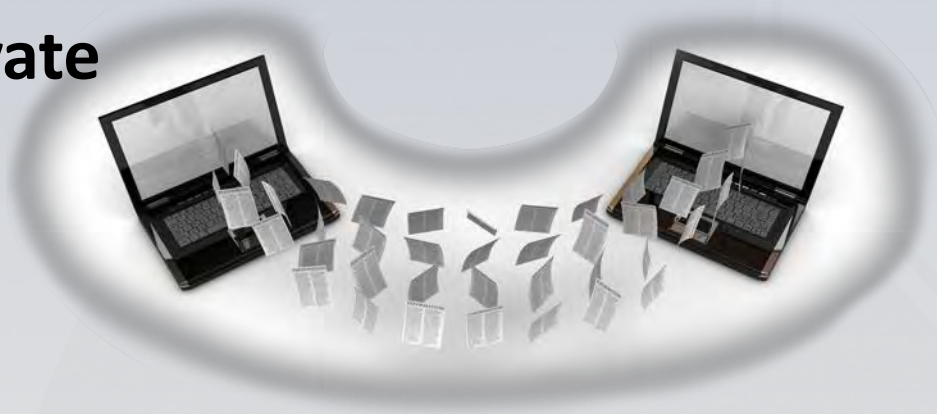
LOCKHEED MARTIN

Threat Information Sharing Journey

- The Road We've Travelled
- Current Landscape
- Navigating for Tomorrow

Why Share Information?

- Drive Intelligence-Driven Defense
- Beyond Indicators & Warnings
- Community Collaboration Expands Feedback Loop
- Builds Trusted Community Partnerships
- Maximizes Public and Private Sector Partnerships



Sharing Leads to Increased National Security

Looking Back (Prior to 2005)

- Broad-based threats were dominant issue
- Government recognition of advanced threat
- Compliance was the measure for security
- Companies have small (if any) CIRT
- Security analysis “outsourced” to AV and IDS vendors

“My antivirus and COTS IDS signature will protect me.”

The Awakening (2005 – 2006)

- **Sophisticated, targeted intrusions impact Public & Private sector**
- **Corporate internal investments ramp up**
- **Information sharing formalizes**
  - Special Access NDAs between industry and LE/CI
  - Air Force partners with industry
  - DoD program specific agreements
  - NDAs develop between several major defense companies

Creating Value through Public & Private Partnerships

Formalization (2007 – 2009)

- **2007– Single, scalable DoD-defense industry partnership takes shape**
  - DEPSECDEF England and DIRNSA brief CEOs of 11 key defense contractors at the Pentagon
  - DIB Cyber Task Force and Defense Collaborative Information Sharing Environment (DCISE)
  - Enables classified-level threat Intel sharing (DIBNET)

- **2008 – Industry-led DSIE for rapid information sharing**
  - Mutual NDA and secure portal enables analyst-to-analyst info sharing, collaboration
  - Quickly has 30+ DIB companies sharing real-time

Success Stories

- Creating real-time situational awareness
- Industry members mature from consumers to producers
- Government and Industry collaboration

Stronger Together through Information Sharing

Public Awareness

- 2005 – Time Magazine, Washington Post first detail APT activity
- 2009 – Google Aurora incident
- 2010 – STUXNET and Details of Buckshot Yankee Release
- 2011 – Numerous incidents reported

Where are we today?

- **Consolidating overlapping information sharing groups**
  - Industry groups integrating (DSIE, NSIE, ADMIE)
  - Government efforts consolidating (CYBERCOM, NCCIC)
  - Public/Private “Kill Chain” analysis workshops
  - Collaboration is faster & broader than ever before
- **Challenges remain**
  - Significant gaps in linking public/private partnerships
  - Multiple government entities establishing “cyber” responsibilities
  - APT focus shifting to supply chain (small to mid sized companies)
  - Cross-sector collaboration

What does the Future bring?

- Legislative/Regulatory Requirements
- Agile Response to Ever Changing Threat Landscape
- Information Sharing Ecosystem

Legislative/Regulatory Changes

- Numerous cyber bills introduced by Congress
- Administration weighing in
- New DFAR Regulations
- Contract clauses to protect unclassified DoD data

Risk of Being Overburdened by Paper Security

Agile Response to Changing Threats

- Moving from information sharing to active blocking
- Security vendors facilitating more intelligence-driven response in tool set
- Targeting of mobile assets
- Adversary Moving from Exploitation to Attacks

Growing Supply Chain Risk

- Attacker shifting focus to smaller companies
- Data stolen from supply chain puts technology at risk
- CNA against supplier disrupts operational capabilities
- Data integrity harder to assure
- Delivery of counterfeit components

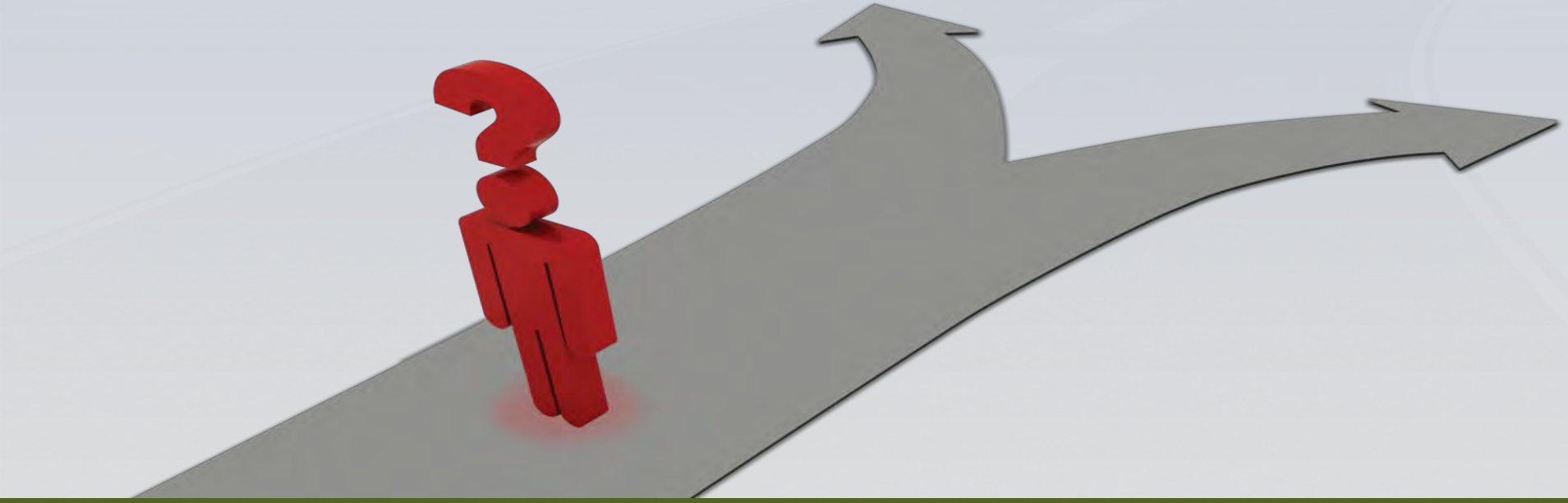
Engaging Supply Chain in Information Sharing Vital to Success

The New Information Sharing Ecosystem

- **Design & Operationalize New Model**
  - Eliminate current challenges
  - Agile & affordable
  - Tiered system
  - Engage broader community

Information Sharing Challenges

- **Avoiding the pitfalls of counterproductive collaboration**
  - Increased OPSEC risks
  - Information dilution, misjudging significance
  - Intelligence echo and negative feedback loop



Shift Threat Sharing Direction

- **Focus on Trusted Information-Sharing "Bridges"**
  - True partnership
  - Government and industry working together
  - Near real-time
  - Formatted data structures
  - Fewer information silos

Enhance Information Sharing Infrastructure to Ensure Future Success

Trusted Bridge Benefits & Approach

- **Benefits**
  - Common understanding of threats & priorities
  - Greater transparency between public & private sectors
  - Greater international information exchange

- **Approach**
  - Smaller companies will need MSSP
  - Data interchange formats enable faster processing
  - Pay-to-play model supports necessary infrastructure

A New Ecosystem

- Continuing Threats
- Richer Partnerships
- Greater Information Sharing

Engagement In Preparedness Resiliency Panel

August 25, 2011

Elusys THERAPEUTICS, INC.

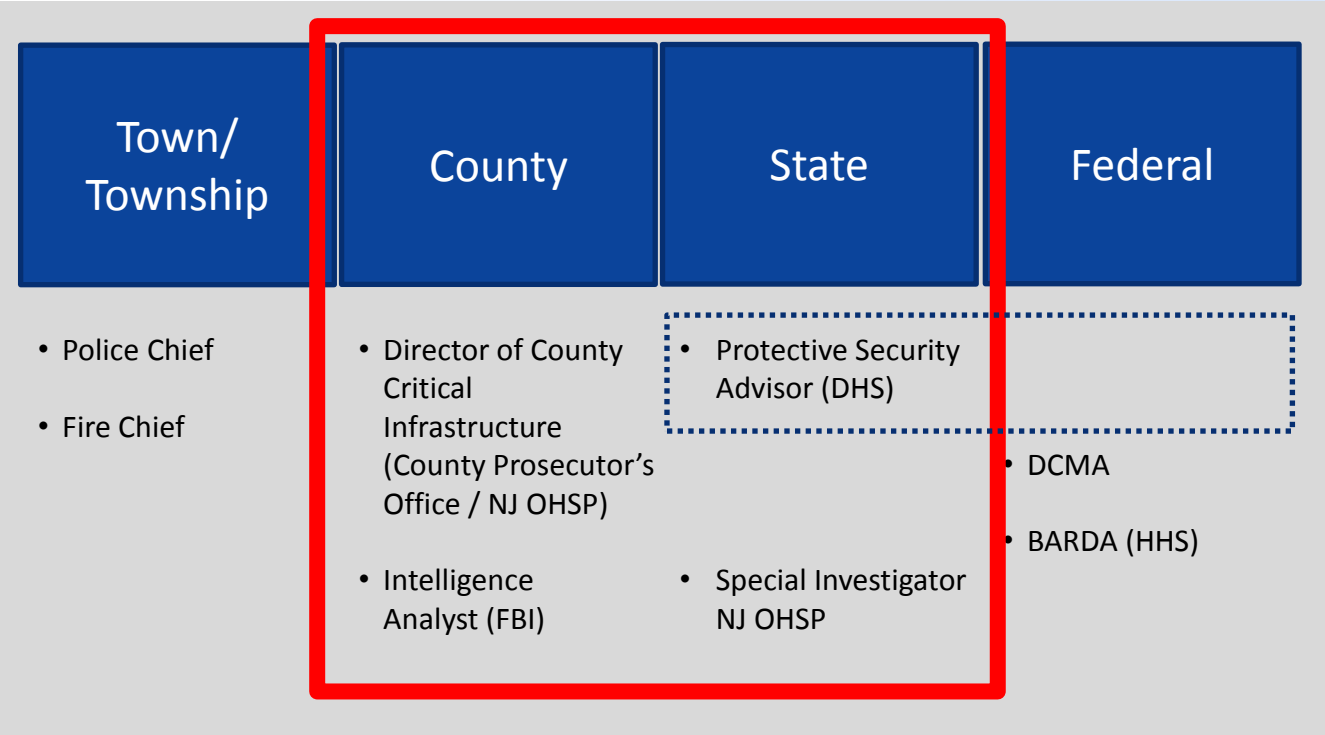
Elusys Therapeutics

- Privately held biotech company based in Pine Brook, NJ
  - < 50 employees
- Primarily focused on the development of Anthim:
  - Anthrax anti-toxin in late stage development
- Prime Contractor to HHS (BARDA and NIAID); DOD
- Engaged in DOD and DHS CIP programs since 2008

Benefit to Elusys

- Identification of Issues and Insights
  - Addressed through business planning processes
    - Reduce overall risk posture
    - Enhance business continuity
- Communication of Best Practices
- Networking

Key Resources for Critical Infrastructure Protection



Defense Security Service

Counterintelligence Directorate

Defense Security Service

DIB CIP Information Sharing Panel

This brief has been produced by the Defense Security Service for DoD contractors and government agencies as part of their security programs. Questions and requests to further distribute this publication should be addressed to the Defense Security Service Counterintelligence Directorate. This document contains information exempt from mandatory disclosure under the Freedom of Information Act.

DSS Counterintelligence Mission

Identify unlawful penetrators of cleared U.S. defense industry and articulate the threat for industry and U.S. government leaders

The Challenge

- DSS responsibility: 8.5K Cleared Defense Contractors (includes 13K facilities)
  - + 24 other agencies
- DSS has approximately 900 FTEs
- DSS CI is authorized 87 FTEs (138 on board)
- DSS supports many Cleared CIP Assets
- Demand for threat information – DSS CI Support – is going through the roof
- Industrial Age capability w/ Info Age challenge
- Secure comm link between DSS & Industry weak

DSS Support to Cleared CIP

- Support in past 12 months to Cleared CIP
  - Multiple fed ops/investigations at DIB Critical Assets
  - DSS tailored threat products for 63% of CIP facilities
  - 100+ IIRs
- DSS CI providing quality feedback/threat info to industry:
  - Feedback on Suspicious Contact Reports
  - Gray Torch Classified Company Assessments
  - Bronze Dragon Classified Program Assessments
  - Threat Info: Annual "Trends," Crimson Shield, Scarlett Sentinel, Threat Advisories, etc
  - Training – "Thwarting the Enemy WBT"
- Collaborating w/ DHS to provide FOUO via HSIN

Desired Capability

- Industry Threat Professionals should:
  - Field skilled threat professionals who know…
    - Threat environment, who poses a threat and reasons if there is no threat reporting
    - Info/technology likely threatened & vulnerabilities
    - How to work the risk equation w/ agility
      - Risk = (Threat + Vulnerability) x Consequence
- DSS CI should:
  - Field a cadre of threat and analysis professionals to assist Industry through action and publications
  - Work the secure communications link issue

Defense Security Service

Counterintelligence Directorate

Questions?

This brief has been produced by the Defense Security Service for DoD contractors and government agencies as part of their security programs. Questions and requests to further distribute this publication should be addressed to the Defense Security Service Counterintelligence Directorate. This document contains information exempt from mandatory disclosure under the Freedom of Information Act.

National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

2011 DIB ★ CIP

DEFENSE INDUSTRIAL BASE CRITICAL INFRASTRUCTURE PROTECTION CONFERENCE

"Setting the Vision and Strategy for the Next Decade"

SUPPLEMENTAL MATERIALS

AUGUST 23-25, 2011

EVENT #1030 ▶ PHILADELPHIA, PA ▶ SHERATON SOCIETY HILL HOTEL

WWW.NDIA.ORG/MEETINGS/1030

Defense Industrial Base

PARTNERSHIP

The Defense Industrial Base (DIB) is one of 18 National critical infrastructure and key resource (CIKR) Sectors and includes hundreds of thousands of domestic and foreign entities and subcontractors that perform work for the Department of Defense (DoD) and other Federal departments and agencies. These firms research, develop, design, produce, deliver and maintain military weapons systems, subsystems, components or parts. Defense-related products and services provided by the DIB Sector equip, inform, mobilize, deploy and sustain forces conducting military operations worldwide. As the Sector-Specific Agency, DoD leads a collaborative, coordinated effort to identify, assess and improve risk management of critical infrastructure within the sector. Members of defense industry associations and DIB private sector critical infrastructure owners and operators form the DIB Sector Coordinating Council (SCC).

VISION

The DIB Sector partnership engages in collaborative risk management activities to eliminate or mitigate unacceptable levels of risk to physical, human and cyber infrastructures, systems and networks, thus ensuring DoD continues to fulfill its mission. DIB activities support national security objectives, public health and safety and public confidence.

GOALS

The following sector goals provide the basis for ongoing risk management activities:

- ***Sector Risk Management:*** Use an all-hazards approach to manage the risk-related dependency on critical DIB assets
- ***Collaboration, Information Sharing and Training:*** Improve collaboration in a shared knowledge environment in the context of statutory, regulatory, proprietary and other pertinent information-sharing constraints and guidance
- ***Personnel Security:*** Mitigate the risk created by personnel with unescorted physical or logical access to critical DIB assets in conformance with pertinent industry best practices, including regulatory and statutory requirements
- ***Physical Security:*** Manage the risk created by threats to and vulnerabilities of critical DIB physical assets
- ***Information Security (Cyber Security/Information Assurance):*** Manage risk to information that identifies or describes characteristics or capabilities of DIB CIKR, or that by its nature would represent a high risk/high impact to the CIKR or DIB assets

DEFENSE INDUSTRIAL BASE GOVERNMENT COORDINATING COUNCIL

The Government Coordinating Council (GCC) is Co-chaired by the DIB Sector Specific Agency (SSA), the U.S. Department of Defense, along with the Department of Homeland Security. These agencies were selected as part of the National Infrastructure Protection Plan (NIPP) as the most highly qualified to protect the CIKR critical to the Nation's defense. The GCC membership also includes leadership from the Departments of:

- State
- Treasury
- Justice
- Defense
- Commerce
- Energy
- Homeland Security

SECTOR COORDINATING COUNCIL COMPANIES/ORGANIZATIONS

- AAI Corporation
- Aerospace Industries Association (AIA)
- Aerojet
- Alliant Techsystems
- American Society for Industrial Security (ASIS) International
- BAE Systems
- Ball Aerospace and Technologies Inc
- Boeing Company

DIB
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
SECTOR COORDINATING COUNCIL

- Booz Allen Hamilton
- Computer Sciences Corporation (CSC)
- DRS, Inc.
- Defense Security Information Exchange (DSIE)
- General Atomics
- General Dynamics
- General Electric
- Honeywell
- Industrial Security Working Group (ISWG)
- L3-Communications
- Lockheed Martin Corporation
- MITRE
- National Classification Management Society (NCMS)
- National Defense Industrial Association (NDIA)
- Northrop Grumman Corporation
- Orbital Sciences
- Pratt & Whitney
- Raytheon Company
- Rockwell Collins
- Rolls Royce
- Science Applications International Corporation (SAIC)
- Textron
- The Analytical Science Corporation (TASC)

SELECTED ACCOMPLISHMENTS

Sector partners continue to maintain and enhance the protective posture of the DIB Sector. Some of the sector's accomplishments over the past year include the following:

- Developed an annual Joint Business Plan (JBP) that focused collaborative efforts to increase DIB Sector resiliency
- Government and Industry representatives established a joint working group to review the DIB criticality process
- Established a DIB network that enabled the electronic communication of classified voice and data information between DoD and participating DIB partners
- Improved processes and expansion plans for the DIB Cyber Security/Information Assurance program and significantly increased defense industry Defense Security Information Exchange (DSIE) membership; UK government and industry officials joined the DSIE
- Deployed a DIB Sector emergency communication notification system
- Improved information sharing by deploying the HSIN DIB SCC portal
- A concise DIB Sector physical security self-assessment tool designed for small and medium size companies was made available on the HSIN DIB portal

KEY INITIATIVES

DoD collaborates with DIB asset owners and operators to develop plans to implement protection recommendations based on the results of risk assessments. Owners and operators make risk-reduction decisions, but DoD strives to facilitate informed decision-making by encouraging information sharing and making decision-support tools available.

Key initiatives within the sector include the following:

- Developing, coordinating and approving the annual listing of DIB critical infrastructure and notifying asset owners and operators of changes in criticality
- Examining and improving the DIB Sector criticality determination and prioritization process
- Establishing and employing business continuity plans for critical infrastructure owner and operator assets

PATH FORWARD

Numerous steps will be taken as the DIB Sector moves forward in securing its resources, including the following:

- Update the JBP among the government and private sector partners, focused on achieving measurable, identifiable results
- Further cooperate with its partners and with sectors that are of critical importance to the DIB Sector, with a focus on interdependencies
- Participate in other related national sector GCCs and working groups
- Partnership for Critical Infrastructure Security and other sector SCCs; and in the State, Local, Tribal, and Territorial Government Coordinating Council and regional working groups;
- Reevaluate sector risk-mitigation activities and metrics to incorporate the results of the joint business plan
- Resolve the issue to "validate" credentials for granting non-employee vendor access to critical facilities in real-time
- Reduce the number of redundant assessments and better coordinate facility site visits by DoD and DHS
- Collaboratively improve critical asset criteria and the determination and prioritization processes

NDIA
National Defense Industrial Association

Sector Annual Report: Defense Industrial Base

EXECUTIVE SUMMARY
JUNE 2010

The U.S. Department of Defense (DoD), the Sector-Specific Agency (SSA) responsible for the Defense Industrial Base (DIB) Sector, and members of the Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) produced the 2010 Defense Industrial Base Sector Annual Report. The report provides progress of the DIB Sector's critical infrastructure and key resource (CIKR) protection and resilience efforts through its 16 risk mitigation activities and fulfills the requirement outlined in Homeland Security Presidential Directive 7 to provide the Secretary of the U.S. Department of Homeland Security (DHS) with the annual report. The report follows the 2010 Sector CIKR Protection Annual Report Guidance issued by DHS.

The DIB Sector is the worldwide industrial complex that enables research and development (R&D), as well as the design, production, delivery and maintenance of military weapons systems, subsystems and components or parts to meet U.S. military requirements. The DIB partnership consists of the DoD and DIB companies that prioritize and coordinate protection and resilience of DIB CIKR.

The DIB faces a growing number of threats and challenges from a wide array of State and non-State actors, including countries operating outside of international norms, criminal organizations, international and "home grown" terrorists and malicious cyber actors. These adversaries may employ creative new approaches to include radicalized or criminal surrogates, manipulating the global economy and information environment, and impeding access to global commodities and supply chains to gain advantage over the U.S. military, allied militaries and supporting industries. A host of primary national security strategy and policy documents, including the 2010 Quadrennial Defense Review Report, reinforce this notion. The most pressing and important risk the sector faces is the cyber threat.

There are five DIB Sector goals and supporting objectives:

- ***Goal 1: Sector Risk Management***. Use an all-hazards approach to manage the risk related to dependency on critical DIB assets
- ***Goal 2: Collaboration, Information Sharing and Training.*** Improve collaboration within a shared knowledge environment set in the context of statutory, regulatory, proprietary and other pertinent information sharing constraints and guidance
- ***Goal 3: Personnel Security.*** Mitigate the risk created by personnel with unescorted physical or logical access to critical DIB assets in conformance with pertinent industry best practices, including regulatory and statutory requirements
- ***Goal 4: Physical Security.*** Manage the risk created by threats to and vulnerabilities of critical DIB physical assets
- ***Goal 5: Information Security (Cybersecurity/Information Assurance).*** Manage risk to information that identifies or describes characteristics or capabilities of a critical DIB asset, or by the nature of the information would represent a substantial risk of adverse impact to the CIKR or the DIB asset

Highlights of progress include a review of prioritized risk mitigation activities of the DIB Sector essential to diminishing the risks and vulnerabilities of the DIB Sector. The 2010 DIB Sector Specific Plan describes in detail 16 risk mitigation activities to improve DIB Sector protection and resilience. Attachment A (not enclosed) describes extensively the risk management activities and performance indicators. The DIB Sector also participates in a number of international activities that it will use and maintain to support DIB sector goals and objectives.

Highlights:

- GCC/SCC and supporting structures (active participation) – meetings/DIB CIP Conference
- 27 awareness visits; 17 assessments
- Began development of standard self assessment tools
- Participation in National Level Exercise 09
- Formed Information Sharing Working Group and identification of baseline information sharing requirements
- Developed an unclassified DIB Network to share information on a DIB pilot company's cyber incidents with DC3
- Continued expansion of the Defense Security Information Exchange
- Sector nominated 3 companies to participate in the Enduring Security Framework
- Conducted first Sector Performance Review

In 2009, the DIB SCC identified four capability gaps: Protection and Prevention; "Ensure Interoperability with the Homeland Security Information Network and Defense Critical Infrastructure Program Common Operating Picture;" Insider Threat Detection; and Entry and Access Portals – "Facilities Access and Credentialing." These capability gaps establish priorities for the DIB Sector's most pressing requirements.

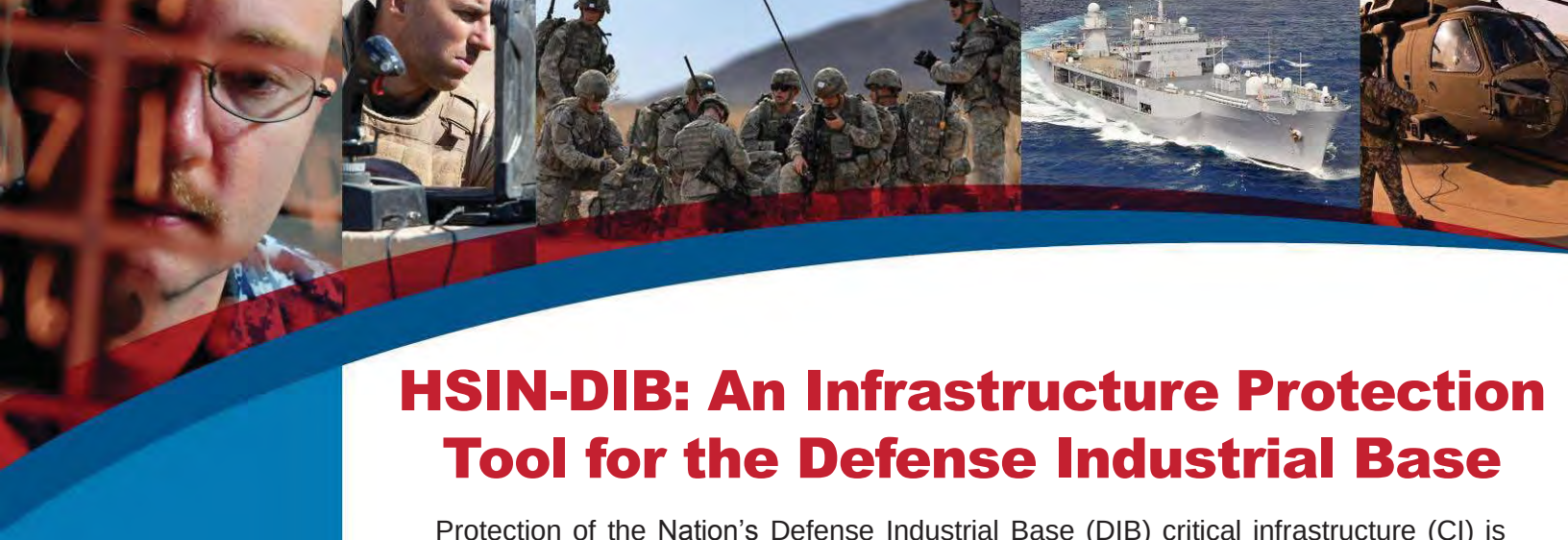
The SSA recognizes the need to develop, manage and coordinate R&D requirements and activities for the DIB Sector. Accordingly, DoD will coordinate with other sectors and academia on the various crosscutting R&D efforts to identify R&D areas beneficial to the DIB Sector and leverage current initiatives underway.

DoD invests in sector protection and resilience programs and activities through a variety of mechanisms. Funding directly targeted at fulfilling DoD's SSA role is $7.7 million in fiscal year (FY) 2010 and $5.2 million in FY 2011.

Finally, this report describes challenges and a path forward agreed upon by the GCC and the SCC and captured in a one-year, joint Business Plan that is focused on five areas:

- Criticality
- Threat Comprehension
- Assessments
- Dependency Analysis
- Information Sharing

This Business Plan will guide joint activity for a one-year period and will be used to evaluate GCC/SCC progress.



HSIN-DIB: An Infrastructure Protection Tool for the Defense Industrial Base

Protection of the Nation's Defense Industrial Base (DIB) critical infrastructure (CI) is essential to maintaining a resilient Nation and fulfilling the National Military Strategy. Collaboration between the public and private sector partners is essential to achieving these goals. HSIN-DIB is one of the primary collaboration tools the DIB public and private sector partners use in support of their joint protection and resilience missions.

What is HSIN-DIB?

The Homeland Security Information Sharing Network for the Defense Industrial Base (HSIN-DIB) is a secure web-based portal which provides vetted Sector members with a gateway to Sensitive But Unclassified (SBU) government and confidential private sector resources for enhancing DIB's protection and resiliency.

HSIN-DIB Features

DIB Public / Private Partnership Collaboration and Resources

Public / Private partners share planning and situational awareness information using various tools including:

- Document Library
- Announcements
- Webinar Tool
- Open Source News Feeds

DIB Private Sector Collaboration and Resources

HSIN-DIB is the designated information sharing platform for the DIB Sector Coordinating Council (SCC) and its various Standing Committees. The portal has a restricted-access area for SCC and private sector partner collaboration, including:

- CounterIntel, Cybersecurity, Info Sharing, Physical Security and Risk Management planning and situational awareness
- Discussion Forums
- SCC and Standing Committee collaboration, including document sharing, action items, etc.
- Calendar of Events

Cross-Sector Collaboration and Resources

Users have access to a wide range of cross-sector SBU resources because HSIN-DIB is part of HSIN-Critical Sectors (HSIN-CS), the Nation's primary Critical Infrastructure Protection information sharing platform. Resources include:

- Event-Specific Information: DHS provides situational awareness for current events and emerging threats
- DHS Content Providers: Access to analysis, intelligence and training products and other CI resources

Request Access to HSIN-DIB

To request access to HSIN-DIB, please submit the following information to CIKRISEaccess@dhs.gov

- Name
- Organization
- Title / Position
- Work email

What can HSIN-DIB help you do?

Share sensitive information openly among trusted community members.

Access timely protection and resiliency information from Members, DHS and other Government organizations using the **Document Library**.

Engage in secure discussions and document sharing with vetted sector peer groups using the **Discussion Board.**

Host virtual presentations, live document review and editing, and live chat with other experts in your field using the **Webinar tool**.

Stay up-to-date on emerging threats and incident information through **Alerts and Notifications**.

How to Access HSIN-DIB

To request access to HSIN-DIB, please submit the following information to cikriseaccess@dhs.gov :

- Name
- Organization
- Title / Position
- Work email

For questions or technical assistance regarding access to HSIN, please contact the HSIN Helpdesk at (866) 430-0162 or send an email to HSIN.helpdesk@dhs.gov.

Vetted users can access HSIN-CS and HSIN-DIB at https://cs.hsin.gov

DEFENSE INDUSTRIAL BASE
GOVERNMENT COORDINATING COUNCIL

DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
SECTOR COORDINATING COUNCIL

SPEAKER BIOGRAPHIES

Introductory Remarks

MG BARRY D. BATES, USA (RET)
Vice President, Operations, NDIA; DIB SCC Chairman

Prior to retirement from the U.S. Army on January 1, 2003, General Bates served as the Commander, 19th Theater Support Command, Eighth U.S. Army, Republic of Korea. In this capacity he was responsible for logistics support and installation management for U.S. Army forces in Korea, as well as for planning wartime logistics to support U.S. Army units deploying to Korea in the event of hostilities.

Previous positions held include Commander, Army and Air Force Exchange Service, Dallas, Texas; G4, Eighth U.S. Army/J4, U.S. Forces Korea / Deputy C4, Combined Forces Command (ROK/U.S.), Republic of Korea; and Vice Commander, Army and Air Force Exchange Service, Dallas, Texas.

During his 32 years of military experience, General Bates has held a variety of command and staff positions in both the continental United States and overseas, serving multiple tours of duty in a joint command environment. He has held both command and staff positions in supply, maintenance and field services organizations, and in the Army's Training and Doctrine Command.

General Bates is a graduate of Oklahoma State University with a B.S. degree in Business and holds an M.S. degree in Logistics Management from the Florida Institute of Technology. He is a graduate of the Industrial College of the Armed Forces and has been recognized as a Certified Professional Logistician by the Society of Logistics Engineers.

General Bates joined NDIA in February, 2003. He and his wife, Laureen, reside in suburban Virginia.

KEYNOTE SPEAKERS
(In Order of Appearance)

Government Keynote Speaker (DoD)

MR. JOSE MAYORGA
DASD Strategy, Force Planning and Mission Assurance, OASD HD&ASA

Mr. Jose Mayorga is the Deputy Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs (Strategy, Force Planning and Mission Assurance). His portfolio encompasses a wide range of responsibilities to include strategy and outreach activities related to information sharing, cyber threat protection, and Department of Defense/Council of Governors initiatives; policy oversight of plans for domestic counterterrorism and counternarcotics activities related to homeland defense and support of civil authorities; and mission assurance policy and activities related to critical infrastructure, defense industrial base and energy grid protection, force protection, and vulnerability assessment. Mr. Mayorga was appointed as DASD on April 25, 2011.

Mr. Mayorga served as the Adjutant General of the State of Texas and was responsible to the President of the United States for providing ready trained forces on federal missions worldwide and responsible to the Texas Governor for providing ready trained forces in support of state emergencies and operations. Mr. Mayorga served in this capacity from April 2009 to March 2011 and was responsible for approximately 25,000 Army, Air, and State Guard service members and State employees. During his tenure as Adjutant General, he deployed approximately 5,000 Army and Air Guard service members to Operations Iraqi Freedom, Enduring Freedom and New Dawn; forged a new State Partnership with the Republic of Chile and continued the enduring State Partnership Program relationship with the Czech Republic; conducted the largest humanitarian assistance joint/combined/interagency exercises in the nation in providing over 55,000 medical services to 13,000 uninsured Texas residents along the U.S./Mexico border in 2009 and 2010; manned and supported six Joint Intelligence Operations Centers in support of local, state and federal law enforcement agencies; executed the President's Southwest Border Mission in deploying 286 service members in support of DHS and Customs and Border Protection; and served on the Adjutant General's Association of the United States, Homeland Security Committee.

Mr. Mayorga was the Commanding General of the 36th Infantry Division from August 2007 to April 2009 and was responsible for the training, readiness, health, and welfare of approximately 17,000 soldiers and their families. He was the principal advisor to the Adjutant General on the use of division resources in support of federal missions and state operations. As Commander of the 36th ID, he trained and deployed over 7,000 soldiers to Operations Iraqi Freedom and Enduring Freedom in addition to deploying over 4,000 soldiers in support of civil authorities during Hurricanes Dolly, Eduard, Gustav, and Ike in 2008 and deploying hundreds more in year-round support for fires, floods, and ice storms.

From September 2005 to August 2007, then Brigadier General Mayorga served as the Deputy Commanding General for U.S. Army South in FT. Sam Houston, Texas. His duties and responsibilities included assisting the Commanding General in prioritizing, planning, and executing over 600 annual operations, exercises, activities and engagements in support of U.S. Southern Command's Theater Security Cooperation Strategy with Central and South America and Caribbean Partner Nations. These events included construction projects, medical readiness exercises, a 20+ nation joint/combined exercise in the defense of the Panama Canal, peace keeping operations exercises, disaster relief/humanitarian assistance exercises, small unit exchanges, subject matter exchanges, and key leader engagements with Army Commanders and Chiefs/Ministers of Defense. Mr. Mayorga was also responsible for assisting the CG in providing T10 Army Executive Agent support to Joint Task Force Bravo in Honduras, Joint Task Force Guantanamo, Forward Operating Base in Colombia, and the Military Groups in over 30 countries within the area of responsibility.

Prior to his promotion to General Officer in 2005, Mr. Mayorga served four years on active duty as an engineer officer in the US Army and had a 24-year civilian career from with the State oil and gas regulatory agency, the Railroad Commission of Texas, as a Petroleum Engineer, District Director, and Assistant Oil and Gas Division Director wherein he was responsible for oil and

gas industry compliance with Commission rules and regulations of approximately 375,000 open oil and gas wellbores across the State of Texas.

Mr. Mayorga earned a Bachelor of Science Degree in Civil Engineering in 1977 from Texas A&I University in Kingsville, TX and a Master of Business Administration Degree in 1989 from Hardin-Simmons University in Abilene, TX. Mr. Mayorga also earned a Master of Strategic Studies Degree in 2001 from the US Army War College in Carlisle, PA. Mr. Mayorga is a Texas Registered Professional Engineer.

Government Keynote Speaker (DHS)

MR. TODD M. KEIL
Assistant Secretary, Infrastructure Protection, DHS

Mr. Todd M. Keil was appointed in December, 2009 by President Barack Obama to serve as the Assistant Secretary for Infrastructure Protection at the U.S. Department of Homeland Security. His office is responsible for protecting the assets of the United States essential to the nation's security, public health and safety, economic vitality and way of life. These assets, referred to as critical infrastructure and key resources, are divided into 18 separate sectors as diverse as agriculture and food, emergency services and critical manufacturing.

Mr. Keil brings to the national infrastructure protection mission more than 22 years of experience in global security operations and management, intelligence and law enforcement and threat assessment and risk mitigation. His recent experience in private industry includes senior consulting in risk mitigation, executive and facility security and worldwide threat management.

Prior to entering private industry in 2007, Mr. Keil held several key positions at the U.S. Department of State's Diplomatic Security Service, including Regional Director for Western Hemisphere Affairs, where he championed protection of U.S. government facilities, personnel and national security information. His responsibilities included oversight of criminal investigations, security training and managing risks from terrorist, criminal and intelligence threats at 56 U.S. Embassies and consulates in the Western Hemisphere, including the U.S. Mission to the United Nations.

In Foreign Service positions in Indonesia, Ireland and Austria, Mr. Keil provided a broad range of security and law enforcement management and risk mitigation expertise, while advising U.S. Ambassadors and in primary liaison roles with a wide network of global law enforcement, intelligence and counter-intelligence agencies. From 1994 – 2000, he held a leadership position on the protective detail that provided personal protection for two Secretaries of State.

Mr. Keil's unique blend of field and high-level management skills and contacts, combined with his expertise in law enforcement, threat and risk assessment and mitigation and applying business best practices to everyday government operations, is an asset to the Department and the mission to protect and build resiliency for the Nation's highly diverse critical infrastructure and key resources.

Mr. Keil holds a Bachelor of Arts in Political Science and Criminal Justice from Ripon College in Ripon, Wisconsin. He has also studied at the University of Bonn in Germany and the American University in Washington, DC. His professional memberships include the Fraternal Order of Police, the American Foreign Service Association and the American Society for Industrial Security.

Mr. Keil is a native of Beaver Dam, Wisconsin, where he attended Wayland Academy.

SPEAKERS & PANELISTS
(In Order of Appearance)

Industry Keynote Panel

MR. CHARLES KOSAK
Principal Director, Homeland Defense Strategy, Force Planning, & Mission Assurance, OASD HD&ASA

Mr. Kosak presently serves as the Principal Director for Strategy and Force Planning in the Office of the Assistant Secretary of Defense for Homeland Defense. He was selected for Senior Executive Service in June 2007.

His previous assignments include Principal Director for OSD Partnership Strategy (3/2008-5/2009), Principal Director for OSD African Affairs (6/2005-3/2008), Deputy Director of OSD NATO Policy (10/2003 to 6/2005), Political Advisor to the Commanding General of V Corps, United States Army Europe (9/1998 to 8/2002), and Senior Policy Analyst on the OSD Balkans Task Force (1/1997 to 8/1998). His deployments while serving the Army include Bosnia, Kosovo, Macedonia, Albania, and Israel.

Mr. Kosak also served as Head of Office for the International Rescue Committee (U.S. NGO) in Mostar, Bosnia and as a Program Officer in Tuzla, Bosnia (9/1993 to 3/1995). Mr. Kosak also served as a Peace Corps Volunteer in the Congo (9/1988 to 1/1991).

His awards include the Secretary of Defense Meritorious Civilian Service Award (2008), the Office of the Secretary ofDefense Group Achievement Award (2008), the Department of the Army Award for Superior Civil Service (2002), the Office of the Secretary of Defense Award for Excellence (2001), the Department of the Army Award for Civil Service (1999), the Office of the Secretary of Defense Award for Excellence (1998), and the Office of the Secretary of Defense Joint Meritorious Unit Award (1998).

Mr. Kosak speaks French and Swahili and enjoys running marathons. He lives in Fairfax, Virginia. He holds a Bachelors Degree from the University of Massachusetts at Amherst (Economics and Political Science) as well as master's degrees from the Graduate Institute of International Studies in Geneva, Switzerland (International P-olitics and Economics) and the National War College, Washington, D.C. (National Security Studies).

MR. IRWIN F. EDENZON
Corporate Vice President, Huntington Ingalls Industries; President, Ingalls Shipbuilding

Mr. Irwin F. Edenzon is Corporate Vice President of Huntington Ingalls Industries (HII) and President of Ingalls Shipbuilding. Named to this position in 2011, he is responsible for all programs and operations at Ingalls Shipbuilding, including U.S. Navy destroyers, amphibious assault and surface combatant programs, and the U.S. Coast Guard cutter program. He also has responsibility for Continental Maritime, a San Diego shipyard that services and supports U.S. Navy ships stationed on the West Coast, and AMSEC, a full-service provider of engineering, logistics and technical support services. Both Continental Maritime and AMSEC are subsidiaries of HII.

Prior to this position and since 2008, Mr. Edenzon served as sector Vice President and General Manager for Northrop Grumman Shipbuilding-Gulf Coast. Prior to this appointment, Mr. Edenzon served as the Director of Future Carrier Programs and as Senior Vice President of Technology Development and Fleet Support for Northrop Grumman Newport News. Named to this position in 2007, he successfully led efforts to increase Newport News' strategic focus on and execution of fleet maintenance business that included surface ships, submarines and commercial ship repair. Prior to joining Northrop Grumman in 1997 as Director of International Programs, Mr. Edenzon was Vice President of Business Development for Textron Marine and earlier served as director of product line and contracts management at Sperry Marine. He began his career in Florida with Perry Offshore, a company that developed and built saturation diving systems, manned submersibles and remotely controlled underwater vehicles for offshore service companies, the U.S. Navy and international navies. During his 10 years with that company, Mr. Edenzon held management positions in business development, contracts and programs.

Mr. Edenzon received a bachelor's degree in Criminal Justice, magna cum laude, from Rutgers University and a master's degree in Business Administration from Florida Atlantic University.

An active member of the community, Mr. Edenzon received the 2009 Outstanding Community Leader of the Year Award for South Mississippi. He is a member of the Gulf Coast Business Council and an Advisory Board Member for the University of Mississippi's Center for Manufacturing Excellence, and he serves on the Board of Directors for Special Olympics of Mississippi. He currently serves as the Chairman of the USO Gulf Coast Advisory Council and is the past Chairman of the USO of Hampton Roads' board of directors.

MR. JOHN JOLLY
Vice President and General Manager, Cyber Systems Division, General Dynamics Advanced Information Systems

Mr. John Jolly, Vice President and General Manager of General Dynamics Advanced Information Systems' Cyber Systems Division, is a twenty-five year veteran of the U.S. Department of Defense and the defense industry. He has an extensive background in program and organization management, strategic planning, financial planning, and technology development.

Mr. Jolly leads an organization that provides best-in-breed systems integration, development engineering and support, cyber situational awareness, digital forensics, and cyber analytics to the Department of Defense, the Intelligence Community, the Department of Homeland Security and Fortune 500 companies. Under his leadership, the Division delivers proven offensive and defensive solutions that harden systems, reduce vulnerabilities, defend against cyber attacks, and enable customer mission success.

Mr. Jolly joined General Dynamics in 2010 after five years in industry providing leadership to a large intelligence-focused business, and previously served for 20 years in the Department of Defense in a variety of program management, technology development and strategic planning roles.

Mr. Jolly is a member of the AFCEA Central Maryland Chapter Board of Directors. He is a member of the Intelligence and National Security Alliance (INSA) and its Cyber Security Council.

Mr. Jolly holds a bachelor's degree with honors in Computer and Information Science from University of Maryland Baltimore County, a master's degree in Program and Organization Management from Johns Hopkins University and a master's in Business Administration with honors from The Wharton School at The University of Pennsylvania.

An Industry Perspective on the Information Sharing Environment of 2020

MS. CHANDRA MCMAHON
Vice President and Corporate Information Security Officer, Lockheed Martin Corporation

Ms. Chandra McMahon was recently named Vice President and Chief Information Security Officer, Enterprise Business Services. In this role, she is responsible for Lockheed Martin's information security strategy, policy, security engineering, operations and cyber threat detection and response. Prior to her current role, Ms. McMahon served as the President of Lockheed Martin Properties, Inc. with responsibilities including corporate real estate, commercial leasing, economic development and facilities management. Prior to the Properties assignment, she served as Program Director for the build and launch of the Center for Leadership Excellence and has held various IT leadership positions in the heritage Integrated Systems & Solutions (IS&S) CIO organization. She currently serves as the executive sponsor of the Corporate Business Resiliency initiative and co-chairs the Lockheed Martin's Women's Leadership Forum.

Ms. McMahon holds a Bachelor of Science degree in Industrial Engineering and Operations Research and a master's degree in Engineering Science, and has earned the designation of PMI's Project Management Professional (PMP).

DIB Cyber Mission Assurance Panel

MR. ROBERT J. GIESLER
Senior Vice President, Cyber Programs, SAIC

Mr. Robert J. Giesler is the Senior Vice President for Cyber Programs, SAIC. Mr. Giesler is responsible for developing corporate-wide strategies, programs, and investments in all facets of the cyber domain.

Prior to coming to SAIC, Mr. Giesler was a member of the Senior Executive Service and served as the Director, Information Operations and Strategic Studies in the Office of the Secretary of Defense.
Mr. Giesler was born in Denver, CO in August 1954, where he completed both elementary and high school. He is a retired Army Officer, having entered the Army in 1972. His Army career included tours in the Infantry, as an Army Counter Intelligence Agent, an Intelligence Operations Officer, and a variety of military operational assignments.

Mr. Giesler's contributions to the Information Operations (IO) and Cyber Operations fields began in 1980 with development and management of unique capabilities directed against strategic targets; participation in the first Information Warfare Net Assessment panel in 1995; and continuous participation in Joint IO and cyber Campaign Plans as either a planner or capabilities provider between 1990 and 2007. He currently consults for the Office of the Secretary of Defense and the Joint Staff on cyber and Information Operations issues, to include serving as the Chairman of a planning Red Team for the Vice Chairman, Joint Chiefs of Staff.

Mr. Giesler is a graduate of the University of Maryland and the Defense Intelligence College Post-graduate Intelligence Program. Among his awards are: The Legion of Merit, the Distinguished Civilian Service Medal, the Meritorious Civilian Service Medal, the Meritorious Service Medal, and the Army Commendation Medal.

MR. CARLOS SOLARI
Vice President, Cyber Technology and Services, CSC

Mr. Solari serves as Vice President, Cyber Technology and Services for CSC. He manages the development of a wide range of cyber solutions, technologies and services related to computer network operations. Among his responsibilities is the overarching management of the development of cyber solutions and services for CSC's customer-facing organizations throughout the public and private sectors.

Mr. Solari has more than 30 years of experience in information technology (IT) and joined CSC from Alcatel-Lucent. While there, he held several senior management roles including Vice President for Security Strategy and Solutions, leading the company's cybersecurity efforts, and Vice President for Quality, Security and Reliability. Previously, Mr. Solari served as the Chief Information Officer at the Executive Office of the President. In this role he developed and implemented the strategy and enterprise architecture for major systems renovation covering all aspects of the enterprise computing serving the White House and its supporting offices. Earlier, he managed several large-scope, full life-cycle IT programs for the Federal Bureau of Investigation.

Mr. Solari is the co-Author of a book on cybersecurity entitled, Security in a Web 2.0+ World (2009) and was selected as a Top 100 Federal Executive by Federal Computer Week in 2004. He holds a Bachelor's degree in Biology from Washington and Lee University, and a Master's degree in Systems Technologies, Joint Command, Control and Communications with an emphasis in Computer Science from the Naval Postgraduate School in Monterey, CA.

Infrastructure Dependencies: The Big Rocks Panel

MR. ROBERT B. STEPHAN
Former Assistant Secretary for Infrastructure Protection, DHS

Colonel Bob Stephan, USAF (Ret) is Managing Director, Dutko Global Risk Management, a core enterprise of the Washington, D.C.-based strategic consulting firm, DutkoWorldwide. Prior to his current position, Colonel Stephan served the Assistant Secretary of Homeland Security for Infrastructure Protection, U.S. Department of Homeland Security from 2005 to 2008. In this capacity, he was responsible for the Department's efforts to catalog our critical infrastructures and key resources, develop the National Infrastructure Protection Plan and coordinate risk-based strategies and protective measures to secure our infrastructures from terrorist attack, as well as enable their timely restoration in the aftermath of natural disasters and other emergencies. His specific areas of focus included the following critical sectors: Transportation (including ports and maritime facilities), Communications, Energy, Dams, Information Technology, Critical Manufacturing, Chemical, Nuclear, Water, Banking and Finance, Food and Agriculture, Commercial Facilities, Government Facilities, Emergency Services, and Monuments and Icons. His efforts also included extensive partnership building and facilitating risk analysis, contingency/resiliency planning, risk mitigation and emergency response planning across a wide array of Federal, State, and local government and private sector security partners.

With the initial activation of the Department of Homeland Security in 2003, Colonel Stephan served as Special Assistant to the Secretary and Director of the Secretary's Headquarters Operational Integration Staff. In this capacity, he was responsible for a wide range of activities that included headquarters-level interaction in the areas of strategic and operational planning, core mission integration, domestic incident management, and training and exercises. He also directed the Interagency Incident Management Group, integrating Department and interagency capabilities in response to domestic threats and incidents.

Previously, Colonel Stephan served as the first Senior Director for Critical Infrastructure Protection in the Executive Office of the President (EOP). During his tenure with EOP, his duties included developing and coordinating interagency policy and strategic initiatives to protect the United States against terrorist attack across critical infrastructure sectors, with a specific focus on the transportation sector.

Colonel Stephan held a variety of key operational and command positions in the joint special operations community during a 24-year Air Force career. During Operation Desert Storm, he deployed to Saudi Arabia as a joint battlestaff planner and mission commander supporting Joint Special Operations Task Force strategic interdiction operations in Iraq. As a Commander of two Air Force Special Tactics Squadrons, Colonel Stephan organized, trained, and equipped forces for contingency operations in Somalia, Haiti, Bosnia, Croatia, Liberia, Colombia, and Kosovo.

Colonel Stephan is a distinguished graduate of the USAF Academy and holds a bachelor's degree in Political Science. He is an Olmsted Scholar and has earned master's degrees in International Relations from the University of Belgrano, Buenos Aires, Argentina, and The Johns Hopkins University.

MR. GUY COPELAND

Vice President, Information Infrastructure Advisory Programs and Special Assistant to the CEO, CSC

As CSC's Vice President for Information Infrastructure Advisory programs, Mr. Copeland is a Special Assistant to CSC's CEO, Michael Laphen, and represents him, in the working bodies of the President's National Security Telecommunications Advisory Committee (NSTAC). Mr. Copeland recently chaired both the NSTAC's Identity Issues Task Force and its Research and Development Task Force. In 2007, he led the formation of and currently serves as one of three co-chairs – two industry and one government – of the Cross Sector Cyber Security Working Group (CSCSWG), an officially recognized, joint government and industry body with over 200 designated representatives from all critical private sector and government coordinating councils. In 2005, he led the formation of and served two terms as the elected first chair of the Information Technology Sector Coordinating Council (IT SCC). He is currently its treasurer and serves on its Executive Committee. He is a Board Member and past President of the Information Technology Information Sharing and Analysis Center (IT-ISAC) which he helped found in 1999. He was a Senior Adviser to the CSIS Commission on Cyber Security for the 44th Presidency and he received a 2008 Federal Computer Week Federal 100 award. Mr. Copeland was a 2005 Senior Fellow at the Homeland Security Policy Institute of George Washington University. A senior member of the IEEE in 1983 – 1984, he was an IEEE Congressional Science Fellow in the office of Senator John Warner. A retired U.S. Army Signal Corps officer, Mr. Copeland's military career included project management, field communications, data network engineering and flying CH-47 helicopters in Vietnam. Mr. Copeland is a dedicated donor (over 330 donations) of platelets, a blood component critical to clotting and essential for transplant operations, cancer treatments and other life threatening emergencies. He has an Master of Science degree in electrical engineering from the University of California, Berkeley and a BS degree in electrical engineering from the University of Wisconsin, Madison.

MR. DOUGLAS OCHSENKENCHT

Mission Assurance Division Head, Naval Surface Warfare Center Dahlgren

Mr. Douglas Ochsenknecht is the Mission Assurance Division Head for the Asymmetric Defense Systems Department at Naval Surface Warfare Center Dahlgren Division (NSWCDD). He is responsible for leading a team of over 100 Civilians providing technical analysis, integration and decision support to the DoD. Mr. Ochsenknecht has over 25 years of experience supporting the United States Department of Defense (DoD) in technical and management positions. Previously, he served as the Program Executive for the Counter-Narcoterrorism Technology Program Office (CNTPO). As the Program Executive for the CNTPO, Mr. Ochsenknecht provided technical and program management leadership to the Counter Narcoterrorism Program and supervised daily operations of the scientists, engineers, contracts and administrative staff of the CNTPO. For FY 08, CNTPO executed approximately $750M of funding with over $2B in awarded contracts. The CNTPO provides global detection, monitoring and disruption of Narcoterroristactivities in support of the DoD strategy. The CNTPO is responsible for developing and applying advanced technology, equipment,and systems to enhance the DoD and, as applicable, the law enforcement communities CNT mission capability. Mr. Ochsenknecht works closely with the Office of the Secretary of Defense, Combatant Commanders, and other government agencies to ensure requirements are met.

Before joining the CNTPO, Mr. Ochsenknecht served as the Technical Director for the Littoral Combat Ship Program at NSWCDD. He provided technical and program management for a diverse team of approximately 60 scientists, engineers and analysts from all technical departments at NSWCDD. Mr. Ochsenknecht directed requirements development, modeling and analysis and the technical evaluation of combat systems, cost, topside design, sensors and weapons selected by the industry teams for the Littoral Combat Ship.

As the Program Manager for Anti Submarine Warfare Combat Systems (ASWCS) at NSWCDD on new construction DDG's (U.S. and Japanese), Mr. Ochsenknecht provided program planning and directed the operations of a team of contractors and Government personnel in the design, review and certification planning for ASWCS. He supported PMS 400 as the Lead Under Sea Warfare (USW) Systems Engineer. PMS 400 was responsible for building and certifying DDG/CG ships. In this role, Mr. Ochsenknecht provided technical and program management oversight for all non-aviation USW systems, both in-service and new construction. He provided Program Management and led the development and certification of all in-service ASWCS baselines. Mr. Ochsenknecht led the implementation of the first digital fire control to torpedo interface on surface ships. This change allowed surface ships for the first time to accurately fire a torpedo without changing course.

Mr. Ochsenknecht worked as the Engineering Services

Department Manager for a defense contractor. He provided Program Management, Systems Engineering, HW and SW development, certification testing, drawings, technical documentation and training for ASW programs to the U.S. NAVY. Prior to this, Mr. Ochsenknecht was a test and evaluation engineer for ASW programs on DD and CG class ships. While attending college at Northeastern University (BSEE 1987), he worked as an engineering Technician on layout, construction and trouble shooting of various circuits. Mr. Ochsenknecht also was a Field Service Representative for on-site testing of nuclear control circuits on TRIDENT Submarines.

MR. BRANDON WALES

Director, Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), DHS

Mr. Brandon Wales is the Director of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and responsible for managing the Center's $40 million budget and approximately 100 threat and risk analysts. Under his leadership, HITRAC has grown from an intelligence-centric organization to a robust, all-hazards analytic resource for public and private sector partners covering the full-array of risks and challenges facing the infrastructure community.

Mr. Wales also oversees the Department's advanced modeling, simulation and analysis program at the National Infrastructure Simulation and Analysis Center (NISAC) where researchers from the Los Alamos and Sandia National Laboratories conduct ground-breaking and forward-leaning analysis of some of the Nation's most complex infrastructure challenges.

When the Department began working on the first Quadrennial Homeland Security Review, Mr. Wales was also asked to lead the review of the counterterrorism and cyber security mission areas.

Prior to joining the Department, Mr. Wales served as the principal National Security Advisor to United States Senator Jon Kyl and as a Senior Associate at a Washington-based foreign policy and national security think-tank.

Mr. Wales received his Bachelor's degree from George Washington University and his Master's degree from Johns Hopkins School of Advanced International Studies.

Information Sharing Panel

MR. TOM WATSON

Director, Infrastructure Coordination and Analysis Office, DHS

Mr. Thomas F. Watson currently serves as the Director of the Infrastructure Coordination and Analysis Office (ICAO) in the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD). The primary responsibilities of ICAO are partnerships, information sharing and knowledge fusion for the protection of Critical Infrastructure and Key Resources Sectors from terrorism and all hazards as directed by Homeland Security Presidential Directive – 7, Critical Infrastructure Identification, Prioritization, and Protection. He supervises a team of senior Sector Specialists who serve as the Critical Infrastructures and Key Resources (CIKR) Sector Coordinators for 12 CIKR Sectors – Agriculture & Food, Banking & Finance, Communications, Defense Industrial Base, Energy, Government Facilities, Health and Public Health, Information Technology, National Monuments & Icons, Postal & Shipping, Transportation Systems and Water. These sectors account for over one third of the nation's economic production.

Prior to joining the DHS, Mr. Watson served on active duty in the U.S. Air Force for 30 years and retired in 2004 as a Colonel. Mr. Watson last assignment was on the faculty of the National Defense University's Industrial College of the Armed Forces in Washington, D.C. During his career in the Air Force, he held a wide range of operations, support and planning positions in strategic airlift.

Mr. Watson is a graduate of the United States Air Force Academy, the United States Army War College, Naval Postgraduate School's Homeland Security Executive Leadership Program and Department of State's National Security Executive Leadership Seminar.

MR. WILLIAM D. STEPHENS

Deputy Program Manager, Office of the Program Manager, Information Sharing Envrionment

Mr. William D. Stephens, a member of the Defense Intelligence Senior Executive Service, is the Director of Counterintelligence, Defense Security Service. He assumed his current position in August 2009.

DSS Counterintelligence (CI) is responsible for providing counterintelligence support to over 13,000 defense contractor facilities employing more than a million cleared personnel. DSS CI identifies the threat posed by foreign intelligence services, their surrogates and other hostile entities and takes appropriate action to protect Department of Defense classified technologies and information resident in the cleared defense industrial base.

Prior to assuming his current position, Mr. Stephens had a distinguished military career, serving in a variety of progressively responsible leadership positions as a special agent and senior field commander with the Air Force Office of Special Investigations (AFOSI). Mr. Stephens retired from the United States Air Force in 2009 after completing his tour as the commander of all AFOSI forces in Europe. He is the recipient of numerous military decorations, including the Defense Superior Service Medal.

Mr. Stephens has extensive practical and managerial experience in CI, both in the field as a special agent and military commander, as well as at programmatic levels, having served in a number of CI-related senior positions on the Air Staff and in the Office of the Secretary of Defense.

Mr. Stephens received a Bachelor of Science degree from Auburn University and possesses three Master of Arts degrees from Central Michigan University, the Naval Post Graduate School and the National Defense University, respectively.

MR. MICHAEL HOWELL

Deputy Program Manager, Office of the Program Manager, Information Sharing Envrionment

On December 6, 2010, Mr. Michael Howell became the Deputy Program Manager of the Office of the Program Manager for the Information Sharing Environment (PM-ISE). The Program Manager has government-wide authority to plan, oversee the build-out and manage use of the ISE to implement the President's terrorism-related information sharing priorities. Mr. Howell's work focuses on assisting the Program Manager in the development of policies, procedures, guidelines, rules and standards to foster the development and proper operation of the ISE while assisting, monitoring and assessing implementation of the ISE by departments and agencies.

Prior to joining PM-ISE, Mr. Howell served as the Deputy Administrator for Electronic Government and Information Technology at the Office of Management and Budget. In that role, he was responsible for overseeing information technology (IT) policy, management and budget for the Federal Government's $80 billion a year IT investment portfolio. He supported the 2008 Presidential transition and the implementation of management reforms and new initiatives to improve IT investment management and the efficiency and effectiveness of Federal IT, open the Government by enhancing transparency and citizen engagement and improve cybersecurity.

Mr. Howell was the Chief Information Officer (CIO) for the Department of the Interior from May, 2007 – September, 2008 providing leadership to the Department and its bureaus in all areas of information management and technology. Mr. Howell served as the Chief Information Officer for the U.S. Fish and Wildlife Service from 2004 – 2007. Previously, he was the Portfolio Management Division Chief in Interior's CIO's Office where he was responsible for overseeing management of the Department's $900 million a year IT portfolio. He served two years as the acting CIO and Deputy CIO for the Bureau of Land Management (BLM) and five years in BLM's headquarters budget office.

Mr. Howell spent four years in BLM's Oregon State Office as a Branch Chief, responsible for software development, Geographic Information Systems, and data and records management programs. Mr. Howell spent seven years in BLM's Eugene District on forest inventory, land use planning and environmental analysis. He worked five years in a variety of forest management jobs in the Medford District in southwest Oregon. His career began in 1978 with the U.S. Forest Service in the Coeur d'Alene National Forest in Idaho and the Olympic National Forest in Washington.

A native of Bethlehem, Pennsylvania, Mr. Howell graduated in 1977 from Pennsylvania State University with a Bachelor of Science degree in Forest Science and a minor in Wildlife Management. In 2005, he completed the Chief Information Officer certification program at the National Defense University IRM College and in 2008 he obtained the Certified Information System Security Professional certificate.

MR. VINCE JARVIE

Vice President, Corporate Security, L-3 Communciations Corporation

Mr. Vincent (Vince) Jarvie is the Vice President, Corporate Security for L-3 Communications Corporation. He is responsible for all aspects of the corporation's global security strategies, processes and operations.

Prior to joining L-3 Communications in October 2005, Mr. Jarvie was the Director of Security with Lockheed Martin Corporation. He served 19 years in numerous security positions with oversight responsibility of Lockheed Martin's Department of Defense, Special Access Program, Sensitive Compartmented Information and Commercial business environment.

Preceding his service with Lockheed Martin, Mr. Jarvie was a special agent with the National Security Agency/Central Security Service (NSA/CSS). He was responsible for the security of NSA/CSS personnel, information and facilities worldwide.

In 2006, Mr. Jarvie was appointed by the Director of the Information Security Oversight Office (ISOO) as a member of the National Industrial Security Program Policy Advisory Committee (NISPPAC). The ISOO is responsible to the President of the United States for policy oversight of the Government-wide security classification system and the National Industrial Security Program; NISPPAC members represent those departments and agencies most affected by the National Industrial Security Program. Also in 2006 he was elected to the Aerospace Industries Association (AIA) Industrial Security Committee, where he currently serves as the Chairman. Mr. Jarvie is the co-Chairman of the FBI National Security Business Alliance Council. Mr. Jarvie is an original Industry member of the Defense Industrial Base Sector Coordinating Council and is the Chairman of the Information Sharing subcommittee.

Mr. Jarvie was awarded the Department of Defense Outstanding Achievement award by the Office of the Secretary of Defense in 2005 for his participation in the development and implementation of the Joint Personnel Adjudication System (JPAS) for Industry. He is also a 2005 recipient of Lockheed Martin's prestigious NOVA award for his leadership and support of the Global Vision Network (GVNet), Lockheed Martin's real-time classified development network for integrated concepts and solutions.

Mr. Jarvie graduated Cum Laude from the University of Maryland with a degree in Criminal Justice. He successfully completed the Carnegie Mellon Executive Leadership and Management graduate program in 2000 and The Wharton School of the University of Pennsylvania, Security Executive Management graduate program in 2007.

Engagement in Preparedness Resiliency Panel

MR. ROBERT READ

Senior Industrial Analyst, OSD AT&L MIBP

Mr. Robert Read is a senior industrial analyst/engineer within the Office of the Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy (MIBP). Mr. Read is the lead action officer for the missiles/munitions and solid rocket motor (SRM) industrial sectors. He also has responsibility for the Defense Critical Infrastructure Program (DCIP) within MIBP. Mr. Read informs Department leaders with accurate and timely industrial information related to decisions that leverage DoD R&D, acquisition, and logistics decisions in order to promote innovation, competition, military readiness, and national security.

Mr. Read came to the Office of the Secretary of Defense (OSD), Pentagon, Washington, DC, in May 1987 as an action officer in the Weapon Support Improvement Group (WSIG) as part of the Assistant Secretary of Defense (Production & Logistics). He developed and assessed DoD reliability, maintainability, and logistics programs for many essential defense space and land warfare programs. He conducted independent logistics engineering and management reviews to support DoD leadership. He performed special studies and assessments that addressed acquisition, logistics, and reliability and maintainability requirements, and feasibility and effectiveness of military service maintenance concepts.
Prior to coming to OSD, Mr. Read spent a year working for the Air Force as a maintainability engineer at the Johnson Space Center in Houston, Texas. He helped develop a standard maintainability process for use by the NASA Space Station program, a common set of maintainability design requirements to be implemented into request for proposals, the interface of maintainability with the integrated logistics support activity and the review and submittal of comments to all NASA Headquarters documents regarding maintainability.

Mr. Read began his government career at Wright Patterson Air Force Base, Ohio, where he provided overall reliability and maintainability engineering support to assigned Air Force program offices (C-17, Air Force One, Advanced Tactical Fighter, F-16C/D, fighter aircraft engines and radar) and laboratories throughout the acquisition process.

MR. JOHN GUEST

IP Regional Director, Mid-Atlantic Region, Protective Security Advisor, DHS

Mr. John J. Guest currently serves as the Regional Director for the Protective Security Advisor Program in the Mid Atlantic Area. He manages ten Protective Security Advisors in Pennsylvania (3), Delaware (1), Maryland (1), Virginia (2), West Virginia (1) and Washington, DC (2). Mr. Guest supports homeland security efforts, serving in an advising and reach-back capacity to state Homeland Security Advisors. He contributes to the development of the national risk picture by assisting with the identification, assessment, monitoring, and minimizing of risk to critical assets at the local level. As the Regional Director, Mr. Guest facilitates, coordinates, and performs vulnerability assessments for local critical infrastructure and assets, and acts as a physical and technical security advisor to Federal, state, and local law enforcement agencies.

Mr. Guest comes to the Department of Homeland Security as an experienced Supervisory Special Agent with the U.S. Secret Service (USSS) with numerous assignments in both protective and investigative divisions. His experience during his 22 years of service included permanent assignments in Philadelphia, PA; Los Angeles, CA; Washington, DC; and Wilmington, DE.

Mr. Guest's protective experience includes a permanent assignment to the Presidential Protective Division where he directed multiple foreign and domestic lead security advances for President Bush and his family. After serving on the Presidential detail, he joined the Technical Security Division where he conducted foreign and domestic technical security advances for both the President and Vice President. Mr. Guest's responsibilities included identifying all hazards associated with explosives, fire, mechanical, and structural integrity, as well as all physical security concerns. Additionally, he developed and implemented security plans and determined appropriate countermeasures including the use of military Explosive Ordnance Disposal bomb technicians, canine resources, and audio countermeasures at designated locations.

Prior to his service with the USSS, Mr. Guest worked with the Philadelphia Fire Department for seven years. After five years as a firefighter in a high-rise district, he was promoted to Lieutenant and assigned as the officer in charge of a Hazardous Material Company.
Mr. Guest holds a Bachelor of Arts Degree in Political Science from Temple University. In 2001, he received a Master of Science Degree in Environmental Protection and Safety Management from Saint Joseph's University. He graduated with honors and was recognized for excellence in service through outstanding scholarship, character and leadership. In 2002, Mr. Guest was appointed as an adjunct faculty member with the Department of Criminal Justice at West Chester University.

Mr. Guest and his wife have two daughters and one son.

MR. JERRY MIDDLETON

Vice President, Corporate Development, Elusys Therapeutics, Inc.

Mr. Jeremy Middleton joined Elusys Therapeutics in May, 2007 and manages corporate development activities, including government affairs, project management, risk management and business development. Mr. Middleton has more than 25 years of management experience in the biopharmaceutical industry at companies including Abbott Laboratories, BASF Pharma and Boots Pharmaceuticals. He holds a Bachelor of Science degree in Applied Chemistry from DeMontfort University in England.

MR. THEODORE M. DAVIDSON

Security and Emergency Services Leader, ULA

Mr. Theodore Davidson currently supports the United Launch Alliance (ULA) as the Leader of Security and Emergency Services. Provide management & oversight for multiple locations in the United States.

Mr. Davidson began working in Aerospace Industry in 1987 as an Industrial Security Representative and has worked in various positions and levels of responsibility with McDonnell Douglas/ Boeing prior to joining ULA.

Mr. Davidson became team member of ULA in January of 2007 and relocated to Denver Colorado.

Education

- Bachelor Degree – Criminal Justice – Long Beach State University – 1986
- Masters Degree – Criminal Justice – Long Beach State University – 1992
- Masters Degree – Organizational Leadership – Chapman University – 2002

MR. RICHARD FORTSON, JR.

Physical Security, Senior Manager, Production Operations, ULA

In Mr. Richard Forston's current role, he is responsible for leading the operations of various security functions including, but not limited to: physical security, fire protection operations, executive protection, crisis management, access management administration, proprietary information protection and destruction, badging, visitor control and security investigations for the Production Operations sites. He has 22 years of Boeing/ ULA security experience.

Prior to joining the company, Mr. Forston served in the United States Army in the elite 1st Cavalry Division Horse Platoon (traveling around the United States re-enacting the old Cavalry on horseback). This unit is a ceremony and recruiting tool for the United States Army. The unit participates in Presidential Inaugural parades, Tournament of Roses Parades and thousands of state local events.

Mr. Forston also served as an Officer for the Travis County Sheriff's Department. While at the Sheriff's Department, he was asked to design and lead the first boot camp on a county level in the nation for convicted offenders. The program was designed for first time convicted offenders who if selected could choose to complete a 180 day boot camp or serve the given sentence in state prison.

Mr. Forston received a Bachelor of Science degree in Business Management from the University of Phoenix.

MS. PAMELA KUCZEK

Risk Manager, ULA

Ms. Pamela Kuczek is the Risk Manager and Business Continuity Leader for United Launch Alliance, LLC. She manages all aspects of insurance programs as well as leads ULA's Business Continuity Program. Pam is an Accredited Business Continuity Planner and Certified Business Continuity Assessor (Standards: BS25999, ASIS SPC 1-2009; NFPA 1600)

Ms. Kuczek joined the ULA team in January 2007. Prior to ULA, she spent over 12 years at Aon Corporation managing complex insurance programs for clients.

MS. CHERRIE BLACK

Bureau Chief, Critical Infrastructure Protection Bureau, New Jersey State Office of Homeland Security and Preparedness

Ms. Cherrie Black is the Bureau Chief for the Critical Infrastructure Protection Bureau in the New Jersey Office of Homeland Security and Preparedness. She has served in that capacity for the Office of Homeland Security and Preparedness and its predecessor, the Office of Counter-Terrorism, since November, 2002. Ms. Black coordinates activities relating to the identification, classification, assessment, prioritization and protection of New Jersey's critical infrastructure. In that capacity, she works closely with the private sector, the U.S. Department of Homeland Security, and state county and local government liaisons. Ms. Black served as a member of the Department of Homeland Security's State and Local Working Group for the National Infrastructure Protection Plan, the Regional Steering Committee for the Radiological Pilot Project Office, and is the State Coordinator for several State and Federal homeland security initiatives. She is the current Vice Chair of the State, Local, Tribal, Territorial, Government Coordinating Council (SLTTGCC) and is Chair of the recently formed SLTTGCC Regional Partnership Working Group. Ms. Black is the former Chair of the SLTTGCC's Chemical-terrorism Vulnerability Information (CVI) Working Group, which provides state and local Government input and recommendations to the Infrastructure Security Compliance Division on protocols and processes for sharing CVI with State and local homeland security officials, law enforcement and first responders. Ms. Black recently served as a State and local subject matter expert on the National Infrastructure Advisory Council's Report and Recommendations on Critical Infrastructure Resilience. An Assistant Attorney General since 2004, Ms. Black served as Chief of the Financial Investigations Unit in the New Jersey Division of Criminal Justice prior to assuming her homeland security responsibilities. As such, she had primary responsibility for implementing the anti-money laundering program and chairing the State Anti-Money Laundering Working Group.

The Future of Response, Recovery and Reconstitution Capability Panel

MR. RICHARD IRWIN

Vice President, Homeland Security and the Intelligence Community, MELE Associates

Mr. Richard Irwin was born on February 6, 1955 in Allentown, Pennsylvania and graduated from York College of Pennsylvania in June 1977 with a B.S. in Police Science. Upon graduation, he began his government career with the Central Intelligence Agency on September 11, 1977. Mr. Irwin's time with the CIA has provided him with extensive operational and senior management expertise specializing in all levels of crisis management, special event planning, physical, technical and operational security, special operations, and counterterrorism, both domestically and overseas. Mr. Irwin's service with the CIA spanned 28 years with assignments in El Salvador, Honduras, Spain, and Italy. He is fluent in Spanish, Italian, and French.

After distinguishing himself in Afghanistan following the September 11, 2001 attacks, Mr. Irwin was assigned to the White House, at the direction of the Director of Central Intelligence, to serve as the Director of Incident Management in the Office of Homeland Security from February 2001 to February 2003. In March 2003, Mr. Irwin was elevated to the position of Director of Incident Management for the Homeland Security Council at the White House, serving in this capacity through May 2004. At the request of Department of Homeland Security Secretary, Tom Ridge, Mr. Irwin was appointed Director of Incident Management for the Department of Homeland Security in June 2004. Mr. Irwin departed the Department of Homeland Security on December 31, 2004, retired from the CIA on March 31, 2005, and began as Vice President of Alutiiq's Homeland Security Division on April 1, 2005.

On January 4, 2010, Mr. Irwin embarked on a new career with MELE Associates as the Vice President of Homeland Security and the Intelligence Community.

Mr. Irwin is married to the former Karen Lynn Peterman of Palmyra, Pennsylvania. They have three children: Kelly, Matthew and Kathleen and reside in Fairfax Station, Virginia. Lastly, Mr. Irwin is the author of KH601 "And Ye Shall Know the Truth and the Truth Shall Make You Free," My Life in the Central Intelligence Agency published by Fortis Publishing in May 2010.

MR. MIKE SMITH

Director, Global Intitiatives, Infrastructure Security and Energy Restoration Division, Office of Electricity and Energy Reliability, DoE

Mr. Mike Smith came to the Infrastructure Security and Energy Restoration (ISER) Division in March 2008 to establish and lead the newly created Global Initiatives Directorate (Directorate). ISER leads a national effort to assure the reliability, survivability, and resiliency of the U.S. energy infrastructure, while also enhancing national energy security by addressing domestic and international energy infrastructure interdependencies. The intent behind this new Directorate was to engage with key energy producing countries and share lessons learned from ISER's years of domestic security experience; helping to assure the continued flow of energy to the United States. In the critical area of Control System Cybersecurity, the Directorate is leading several domestic and international efforts to address cyber vulnerabilities in the Energy Sector.

Mr. Smith also established the Department's Combatant Command (COCOM) Energy Advisor program, hiring and deploying a DOE Energy Advisor to each COCOM headquarters. These Energy Advisors provide comprehensive strategic energy support to the COCOM leadership, to include analysis and reporting, as well as critical reach back to DoE national laboratories. The first DoE Energy Advisor deployed to Africa Command in July 2009, followed by Central Command in June 2010, Southern Command in July 2010, European Command in September 2010, and Pacific Command in August 2011.

Prior to coming to DoE, Mr. Smith was a consultant with Booz Allen Hamilton for four years. He supported a variety of Department of Defense (DoD) clients, the last of which was the Defense Critical Infrastructure Program (DCIP) Office. Mr. Smith advised the DCIP Director on all international infrastructure sectors, primarily focusing on the Defense Industrial Base, energy, and telecommunications. He was the DCIP lead on DOD's Global Information Grid Support to Mission Assurance Task Force and managed the Committee on Foreign Investment in the United States program. Before coming to the DCIP office, Mr. Smith supported the DoD Chief Information Officer's Information Assurance Division, providing policy and technical expertise in identifying, analyzing and mitigating the risks posed to DoD information networks by the globalization of the information technology and telecommunications supply chains.

Mr. Smith retired from the U.S. Army's Judge Advocate General's Corps in January 2004. During his 16 year career, he served in a variety of assignments around the world, to include: deploying with 1st Armored Division to Operations Desert Shield/Storm; Litigation and Defense Appellate Attorney in Washington DC; Fort Bragg, North Carolina, where he served two years on jump status as Chief, Operational Law, XVIII Airborne Corps; and Korea as the 2d Infantry Division Deputy Staff Judge Advocate. After Korea, Mr. Smith returned to Washington DC as the Army Operations Center Legal Advisor in the Pentagon, where he was working on the morning of September 11, 2001.

Mr. Smith was born in Burbank, California, and grew up in San Diego. He graduated from the University of Oklahoma with a BA (1983) and a JD (1987) and Georgetown University Law Center, where he earned a Masters of Law in International and Comparative Law (1999).

He and his wife, Susan, live in Fairfax, Virginia. They have two grown daughters and a son in college. Mr. Smith and Susan are avid golfers.

DR. THOMAS BOGDAN

Director of the Space Weather Predition Center, NOAA, DoC

Dr. Thomas Bogdan has been the Director of the National Oceanic and Atmospheric Administration's Space Weather Prediction Center, located in Boulder, Colorado, since May of 2006. In this capacity, he serves as the principal

representative for civil space weather operations in the United States and is the national liaison to the World Meteorological Organization for space weather matters. He is also a co-Chair of the multi-agency National Space Weather Program.

The Space Weather Prediction Center is the official source for our Nation's space weather prediction, forecast and warning services. It operates 24/7 with a yearly budget of $9 million and is one of only four Department of Homeland Security-designated National Critical Systems in the National Weather Service. Approximately 50 civil servants and a dozen contractors work to provide space weather guidance that is critical for (i) the aerospace industry, (ii) our homeland security and national defense, (iii) Global Navigation Satellite Services, (iv) commercial aviation and (v) the integrity of the power grid.
A Fellow of the American Meteorological Society, Dr. Bogdan was previously a senior scientist and an administrator with the National Science Foundation (NSF) sponsored National Center for Atmospheric Research (NCAR), from 1983 – 2006. There, he carried out fundamental research on solar magnetic activity, led the Societal Environmental Research and Education Laboratory and directed NCAR's prestigious Advanced Studies Program. Between 2001 and 2003, Dr. Bogdan served as the Program Director for the Solar-Terrestrial Research Section of NSF's Atmospheric Sciences Division. During this time, he was instrumental in developing the NSF's first bridged faculty program in the space sciences that resulted in the creation of eight new tenure track faculty lines devoted to solar-terrestrial research and education at several major U.S. universities.

Dr. Bogdan earned his Doctorate in Physics at the University of Chicago in 1984 and graduated Summa Cum Laude with a B.S. in mathematics/physics from the State University of New York at Buffalo in 1979. He is the Author of over 100 papers in solar-terrestrial research, was the recipient of the Gregor Wentzel and Valentine Telegdi Prizes from the University of Chicago. He spent the summer of 1989 as a Visiting Gauss Professor at the Universitäts Sternwarte in Göttingen.

NDIA
National Defense Industrial Association

ATTENDEE ROSTER

As of 8/16/2011

Mr. Daniel Abreu
DHS Office of Infrastructure Protection

Mr. Michael Adams
NSWC PCD

Mr. Peter Adler
SRA International

LtCol John Allison, Sr., USMC (Ret)
IST Research

Ms. Mayra Alvarado-Rivera
DoD, Office of the Inspector General

Mr. Dennis Arriaga
SRI International

Mr. George Atkinson
SAS Institute, Inc.

MG Barry Bates, USA (Ret)
NDIA

Ms. Lisa Bendixen
ICF International

Ms. Cherrie Black
NJ Office of Homeland Security & Preparedness

Dr. Thomas Bogdan
DoC

Mr. Adam Bonanno
The SI Organization, Inc.

Mrs. Diane Brooks-Woodruff
Defense Security Service

Mr. Chris Burmeister
Lockheed Martin Corporation

Ms. Rosemarie Burnett
DCMA - Industrial Analysis Center

Mr. Ryan Byrd
Argy, Wiltse & Robinson, PC

Hon. Chris Carney
BAE Systems

Mr. Jake Carson
U.S. Transportation Command

Mr. William Carwile
FEMA

Mrs. Bobbi Castanon
Lockheed Martin Information Systems & Global Solutions

Mr. Frédéric Chartrand
Department of National Defence

Ms. Leda Chong
General Dynamics Corporation

BG Ken Chrosniak, USA (Ret)
U.S. Army War College

Mr. Jamie Clark
DoE

Mr. Larry Clark
HQ Department of Army G-3/5/7

CAPT Richard Cline, USN (Ret)
Lockheed Martin Information Systems & Global Services

Mr. Stephen Colo
SAIC

Mr. David Compton
Naval Criminal Investigative Service

Mr. Jim Connelly
Lockheed Martin Corporation

Mr. Mark Connelly
ITT Defense

Mr. Guy Copeland
CSC

Mr. Thom Covington
The Boeing Company

Mr. Ted Davidson
ULA

Mr. Allen Davis
DoD, Office of the Inspector General

Mr. Ron Davis
BAE Systems

Mr. Michael Dietz
HQ USEUCOM

LTC Bob Domenici, USA (Ret)
Strategic Response Initiatives, LLC

Mr. Bill Donaldson
National Center for Crisis and Continuity Coordination

Mr. Mike Donnelly
National Center for Crisis and Continuity Coordination

Mr. Derek Dunaway
Cyalume Light Technology

Mr. Jason Dury
SAIC

Ms. Alice Dysart
Alice Dysart, Inc.

Mr. Gerard Eaton
Looking Glass Cyber Solutions, LLC

Mr. Irwin Edenzon
Ingalls Shipbuilding

Mr. Bill Ennis
Ennis Strategic Enterprises

Mr. Mark Evans
URS Corporation

Ms. Lori Feliciano
Office of the Director of National Intelligence

Mr. Al Ferzacca
Sandia National Laboratories

LtCol Juan Figueroa, USMC (Ret)
DHS

Mr. Richard Fortson, Jr.
ULA

Mr. Doug Frank
BAE Systems Global Tactical Systems

LTC Steve Frankiewicz, USA (Ret)
ITT Information Systems

Mr. Jonathan Fraser
Defense Security Service

Mr. John French
TSA - Pipeline Security Division

Mr. Scott Gane
General Atomics

Mr. Robert Giesler
SAIC

Mr. Brendan Glasgow
SafeNet, Inc.

Mr. John Glowa
The Boeing Company

Mr. Rick Graham
Huntington Ingalls Industries

Mr. Ryan Gray
KBR

Col Joe Guirreri, USAF (Ret)
PESystems, Inc.

Ms. Alison Hafer
DCMA - Industrial Analysis Center

Mr. David Hagy
OASD HD&ASA

Lt Col Monty Hand, USAF (Ret)
HQ USAFE/A3J

Maj Gen George Harrison, USAF (Ret)
GA Tech Research Institute

Mr. John Hashem
OASD CHD&ASAJ

Mr. Martin Hembree
NSA

MSG Paul Herd, USA (Ret)
NORAD USNORTHCOM

Col Steve Heuer, USAF (Ret)
USTRANSCOM

Mr. Neil Holloran
NSWC Dahlgren

Mr. Michael Howell
Information Sharing Environment

Mr. Sean Howley
ICF International

Mr. Travers Hurst
Oak Ridge National Laboratory

Mr. Russell Ignarro
DHS

Mr. Richard Irwin
MELE Associates, Inc.

Mr. Alex Ivanchishin
ANSER

Mr. Vincent Jarvie
L-3 Communications Corporation

Mr. Derek Jenkins
Huntington Ingalls Industries

Mr. Dave Johnson
Joint Staff J-34

Mr. David Jones
DCMA - Industrial Analysis Center

Dr. Nathan Kathir
HQ U.S. Army Corps of Engineers

Mr. Matt Keck
Lockheed Martin Corporation

Mr. Todd Keil
Protection HQ DHS

Mr. Mike Kennelly
Raytheon Missile Systems

Mr. Michael Knee
The Boeing Company

Mr. Chuck Kosak
OASD HD&ASA

Ms. Pam Kuczek
ULA

Mr. Bill Kutz
Lockheed Martin Corporation

Mr. Tom LaCrosse
DHS

Dr. Mark Leary
TASC

Ms. Vivian Linder
Becatech, Ltd.

Mr. Steve Lines
SAIC

Mr. Eugene Marrone
DCMA - Industrial Analysis Center

Mrs. Amy Mathews
DoD, Office of the Inspector General

Mr. Chris Mathieu
BAE Systems Mobility & Protection Systems

Mr. Dirk Maurer
MacAulay Brown, Inc.

Mr. Jose Mayorga
OASD HD&ASA

Mr. Bob McCants, Jr.
SRA International

Mr. Scott McCoy
ATK

Mr. Brad McGowan
The Spectrum Group

Mrs. Chandra McMahon
Lockheed Martin Corporation

Mr. Tim McMillan
Lockheed Martin Corporation

Mr. Jeremy Middleton
Elusys Therapeutics, Inc.

Mr. Mark Milicich
DHS, Office of Infrastructure Protection

Capt Ed Miller, USAF (Ret)
Raytheon Missile Systems

Ms. Gail Miller
DELTA Resources, Inc.

Mr. Jeff Miller
Honeywell

Mr. Praveen Money
Honeywell

Mr. Reginald Moore
Resource Management Concepts, Inc.

Mr. Edward Morehouse
OSD AT&L

MAJ John Morris, USA
U.S. Army

Mr. Mark Murphy
CACI, Inc.

Mr. Ray Musser
General Dynamics Corporation

Mr. Simon Narborough
American Shipping & Logistics Group

Mr. Mike Nemeth
Zyvex Performance Materials

Mr. Michael Nicolas
Huntington Ingalls Industries

Mr. Pat Nigro
Deloitte Financial Advisory Services, LLP

Mr. Douglas Ochsenknecht
NSWC Dahlgren

Mr. Leo O'Shea
URS Corporation

Ms. Mysia Pallas
DLA

Mr. Greg Pannoni
NARA

Ms. Patricia Passarella
DCMA - Industrial Analysis Center

Mr. Tim Patterson
CACI, Inc.

Mr. Roland Perry
DoD IG

Mr. Joe Pipczynski, Jr.
Telephonics Corporation

Mr. Malik Powell-Hodge
DoD IG

Mr. Steve Pranger
HQ U.S. Army Corps of Engineers

Ms. Danica Quigley
Personnel and Readiness Information Management

Mr. Burt Quist
Northrop Grumman Corporation

Mr. Bob Read
OSD AT&L MIBP

Mr. Rick Read
Lockheed Martin Corporation

Mr. Nick Reves
CENTRA Technology

Mr. Mario Riggione
SAIC

Mr. Scott Riney
SRA International

Mr. Jim Russell
QinetiQ North America

Mr. Scott Rutler
Booz Allen Hamilton

LCDR Dave Ryan, USN
Assistant Secretary of the Navy (Energy, Installations and Environment)

Mr. John Schauffert
U.S. Northern Command J34 (Force PROT, Mission)

Ms. Brittany Schick
Booz Allen Hamilton

Mr. Todd Sherwood
National Geospatial-Intelligence Agency

Mrs. Vicki Short
OSD

Mr. Andrew Smith
NJ Office of Homeland Security & Preparedness

Mr. Frank Smith
Booz Allen Hamilton

Ms. Hanifa Smith
DoD

Ms. Hillary Smith
DoD, Office of the Inspector General

Mr. Mike Smith
Infrastructure Security & Energy Restoration

Mr. Eric Sobota
Argy, Wiltse & Robinson, PC

Mr. Carlos Solari
CSC

Mr. Bob Sommers
NORAD USNORTHCOM

LTC Dixie Southerland, USA (Ret)
BAE Systems

Ms. Karen Stence
NSWC PCD

Mr. Bob Stephan
Dutko Worldwide

Col William Stephens, USAF (Ret)
Defense Security Service

Dr. Paul Stockton
OASD HD&ASA

Mr. Simon Stringer
Becatech, Ltd.

COL Jack Summe, USA
OSD Cyber Policy

Mr. Bob Summers
National Nuclear Security Administration - Nevada

Ms. Saundra Throneberry
Lockheed Martin Corporate Engineering

Mr. Michael Titone
DIB Cyber Security/Information Assurance Program Office

Mr. Bill Toth
QinetiQ North America

Mr. Larry Trittschuh
General Electric Company

Mr. Steve Turdo
DCMA - Industrial Analysis Center

Mr. CJ Unis
Sandia National Laboratories

Mr. Dan Van Belleghem
NCI Information Systems, Inc.

Mr. John Viar, Jr.
SPEC Innovations

Mr. Jim Vreeland
Huntington Ingalls Industries

Mr. Brandon Wales
DHS

Mr. Tom Watson
DHS

Ms. Kristen Weghorst
Lockheed Martin Information Systems
& Global Solutions

Mr. Phil White
Assured Information Security, Inc.

Mrs. Claire Willette
Strategy, Force Planning & Mission
Assurance

Mr. Ray Williams
L-3 Communications Corporation

Col Carl Williamson, USAF (Ret)
Northrop Grumman Corporation

Mr. Kevin Winter
SRA International

Col Mike Witt, USAF (Ret)
Ball Aerospace & Technologies Corp.

Ms. Kelly Woods Vaughn
Metters Industries, Inc.

Mr. Brent Wrisley
SRA International

Mr. Joseph Zagrapan
Radford Army Ammunition Plant

Mr. Jeff Zimmerman
CSC

THANK YOU TO OUR SPONSORS!

CACI

EVER VIGILANT

ICF

INTERNATIONAL