2010 Defense Industrial Base Critical Infrastructure Protection Conference (DIBCIP)

“Risk Reduction & Mitigation in the Defense Industrial Base”

April 26-28, 2010
Philadelphia, PA

Agenda

Tuesday, April 27, 2010

Keynote Address: The Economic Crisis and Its Impact on the DIB: Defense Industrial Base Forecasts 2010-2020
- Mr. James Averell, Economist, DCMA-Industrial Analysis Center

Panel: Cyber Security Critical Infrastructure Protection and Public-Private Partnerships
- Mr. Steve Lines, Director, Business Continuity and Information Assurance, Science Applications International Corporation (SAIC); DSIE Chairman
- Mr. Guy Copeland, Vice President of Information Infrastructure Advisory Programs within Computer Science Corporation’s North American Public Sector; CSCSWG Co-Chairman

Panel: Critical Infrastructure Protection Mission Assurance Assessments (MAA)
- Mr. Steve Turdo, Industrial Specialist, DCMA Lead CIP-MAA Analyst, DCMA-Industrial Analysis Center
- BG James Hoyer, USA, Director, Joint Staff, WV Army National Guard

Wednesday, April 28, 2010

Industry Keynote Address
- Mr. Ed Halibozek, Director of Corporate Security, Northrop Grumman Corporation

Threats to the DIB
- Ms. Melissa Smislova, Associate Deputy Under Secretary for Analysis (DU/S-A), U.S. Department of Homeland Security

Panel: Interdependencies Risk Management
- Capt. Walt Smith, Philadelphia Police Department, Homeland Security Division
- Mr. Lawrence V. Wasnock, Vice President, Human Resources & Ethics Officer, L-3 Communications - Marine & Power Systems
- Mr. Jake Carson, Program Manager, U.S. Transportation Command
- Mr. Christopher Reichart, Head, Infrastructure & Networks Analysis & Assessment Branch, Naval Surface Warfare Center-Dahlgren Division, Z32

Panel: DIB Sector Involvement in Recent and Planned Exercises
- COL Paul Ahern, USA, Director, Response Team, DCMA- Industrial Analysis Center
- Mr. John Schaufert, Assessments Branch Chief, Force Protection and Mission Assurance Division, U.S. Northern Command,
- Ms. Nancy Pomerleau, Exercise Director, Partnership Outreach Division, DHS-IP DIB

-
2010 DIB★CIP
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION CONFERENCE

“Risk Reduction & Mitigation in the Defense Industrial Base”
MONDAY, APRIL 26, 2010

12:00-7:30pm	 Registration
6:00-7:30pm	 Networking Reception

TUESDAY, APRIL 27, 2010

7:00-5:00pm	 Registration
7:00-8:00am	 Continental Breakfast
8:00-8:15am	 Welcome & Introduction
• MG Barry D. Bates, USA (Ret), Vice President, Operations, NDIA; DIB SCC Chairman
• Mr. Jamie Clark, Director, Defense Critical Infrastructure Program, Office of the Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs; DIB GCC Chairman
8:15-9:15am	 Keynote Address
• Honorable Dr. Paul Stockton, Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs
9:15-10:15am	 Senior Level Discussion on Infrastructure Protection
• Mr. Todd Keil, Assistant Secretary, Office of Infrastructure Protection, U.S. Department of Homeland Security
Discussion Topics: Challenges and efforts relating the protection of assets essential to the nation’s security, public health and safety, economic vitality and way of life.
10:15-10:45am	 Networking Break
10:45-12:00pm	 Panel: Resilience Leadership
• Mr. Michael C. H. McDaniel, Deputy Assistant Secretary of Defense for Homeland Defense Strategy, Prevention & Mission Assurance, DoD
• Mr. Raymond Musser, Staff Vice President - Security, General Dynamics; DIB SCC Vice Chairman
• Ms. Carolyn Parisot, FBI
• Mr. Darrell Darnell, Director, Critical Infrastructure Protection and Resilience Policy, National Security Staff, The White House
Discussion Topics: Critical Infrastructure Protection activities affecting DIB sector resiliency; Visions for the future.
12:00-1:00pm Networking Buffet Lunch

1:00-2:00pm Keynote Address: The Economic Crisis and Its Impact on the DIB: Defense Industrial Base Forecasts 2010-2020
   • Mr. James Averell, Economist, DCMA-Industrial Analysis Center

2:00-3:15pm Panel: Cyber Security Critical Infrastructure Protection and Public-Private Partnerships
   • Mr. Thomas Bozek, Principal, Bozek Consulting, LLC
   • Mr. Steve Lines, Director, Business Continuity and Information Assurance, Science Applications International Corporation (SAIC); DSIE Chairman
   • Mr. Guy Copeland, Vice President of Information Infrastructure Advisory Programs within Computer Science Corporation’s North American Public Sector; CSCSWG Co-Chairman
   • Mr. Brian Fredericks, Deputy, DIB CS/IA Task Force, OASD (NII)
   • Mr. Eric Noonan, Director of Security, BAE Systems

Discussion Topics: Defense industry efforts to combat the attacks of cyber warfare; The mission and activities of the Defense Security Information Exchange; Public-private partnerships; National level issues, initiatives and activities of the working bodies of the President’s National Security Telecommunications Advisory Committee (NSTAC).

3:15-3:45pm Networking Break

3:45-5:00pm Panel: Critical Infrastructure Protection Mission Assurance Assessments (MAA)
   • Mr. Steve Turdo, Industrial Specialist, DCMA Lead CIP-MAA Analyst, DCMA-Industrial Analysis Center
   • Col Thomas McGinley, USAF, Provost Marshal J34, National Guard Bureau
   • Mr. Justin Rubin, Business Continuity Coordinator, BAE Systems Electronic Solutions
   • BG James Hoyer, USA, Director, Joint Staff, WV Army National Guard
   • MAJ Scott White, USA, CIP-MAA Team Leader, NY Army National Guard
   • 1LT Jeremy Samples, USA, CIP-MAA Team Leader, WV Army National Guard, JITEC
   • 1SG Jon Huddleston, USA, CIP-MAA Team Sergeant/Mission Analyst, CO Army National Guard

Discussion Topics: Overview and demonstration of DoD CIP-MAA purpose and process; Trend analysis and mitigation strategies for common vulnerabilities within the sector.

5:00pm Adjourn for the Day
WEDNESDAY, APRIL 28, 2010

7:00-5:00pm  Registration

7:00-8:00am  Continental Breakfast

8:00-9:00am  Industry Keynote Address
• Mr. Ed Halibozek, Vice President of Security, Flight Operations and Administration, Northrop Grumman Corporation


9:00-10:00am  Threats to the DIB
• Ms. Melissa Smislova, Associate Deputy Under Secretary for Analysis (DU/S-A), U.S. Department of Homeland Security

Discussion Topics: A general threat overview for current activities within the last 6-9 months with a focus on matters important to the Defense Industry; Perspectives on the effectiveness of public/private sector information sharing practices and a vision for improving information sharing capabilities in the future.

10:00-10:30am  Networking Break

10:30-12:00pm  Panel: Homeland Defense/Security/Local Program Implementation - Effective Partnerships
• Mr. Raymond Musser, Staff Vice President - Security, General Dynamics; DIB SCC Vice Chairman
• Chief William McSweeney, Los Angeles Sheriff, Homeland Security Division
• Sgt. Peter Jackson, Los Angeles Sheriff’s Department, Joint Regional Intelligence Center
• Ms. Kathy McKeever, Assistant Deputy Director, Critical Infrastructure Protection, California Emergency Management Agency

Discussion Topics: Ongoing and planned activities, success stories and challenges with implementing comprehensive preparedness, response and recovery tactical programs operations in major metropolitan areas by building effective partnerships with the federal government, regions, state governments and the defense industry.
12:00-1:00pm  Networking Buffet Lunch

1:00-2:30pm  Panel: Interdependencies Risk Management

- Ms. Mary Ann Tierney, Deputy Managing Director for Emergency Management, Philadelphia
- Capt. Walt Smith, Philadelphia Police Department, Homeland Security Division
- Mr. Lawrence V. Wasnock, Vice President, Human Resources & Ethics Officer, L-3 Communications - Marine & Power Systems
- Mr. Jake Carson, Program Manager, U.S. Transportation Command
- Mr. Christopher Reichart, Head, Infrastructure & Networks Analysis & Assessment Branch, Naval Surface Warfare Center-Dahlgren Division, Z32

Discussion Topics: Improving government communication, analysis and coordination for DIB CIKR dependent systems to enhance the overall resiliency of the sector; A discussion of typical dependencies and what government and industry are doing to mitigate risks.

2:30-3:00pm  Networking Break

3:00-4:30pm  Panel: DIB Sector Involvement in Recent and Planned Exercises

- COL Paul Ahern, USA, Director, Response Team, DCMA-Industrial Analysis Center
- Mr. John Schauffert, Assessments Branch Chief, Force Protection and Mission Assurance Division, U.S. Northern Command, J34
- Mr. David Kemeter, Lead, Planning and Preparedness, DCMA-Homeland Defense
- Mr. Robert Connors, Preparedness Director, Raytheon Company
- Ms. Nancy Pomerleau, Exercise Director, Partnership Outreach Division, DHS-IP DIB

Discussion Topics: Lesson learned and activities planned for upcoming exercises; DIB sector involvement in recent and planned exercises; Raytheon’s preparedness planning and participation in national and local area exercises.

4:30-5:00pm  Closing Remarks

- Mr. Jamie Clark, Director, Defense Critical Infrastructure Program, Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs; DIB GCC Chairman
CSC has an unparalleled ability to solve the critical cyber challenges our clients face. Our cybersecurity solutions are built upon an in-depth understanding of IT vulnerabilities, knowledge of cyber enemies, and proven experience building and managing enterprise networks and systems. As a trusted leader in cyber solutions around the world, CSC protects some of the nation’s—and the world’s—most sensitive information, systems and networks.

Drawing on our 50 years of expertise and experience, we help organizations achieve a new competitive advantage in the marketplace. Our deep understanding of cyber complexities that cover the entire cyber spectrum gives our clients the assurance they need to take action, mitigate risks and realize their full potential in this digital economy.

Our Defense Industrial Base—Security Assessment Report (DIB-SAR) solution allows contractors to address the ever changing threat environment and quickly evolving Department of Defense regulations for controlled, unclassified information programs and technologies. CSC helps DoD contractors to get a better understanding of their overall security posture and meet security requirements necessary to host CUI data. The DIB-SAR solution suite consists of three services: DIB-SAR assessment, infrastructure build-out of a corporation’s IT environment to cover gaps determined in the assessment, and an executive report identifying areas of compliance with FISMA and NIST standards.

For additional information, please visit: http://www.csc.com.
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, a donation has been made to the Wounded Warrior Project.

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

SURVEY
A survey will be e-mailed to you after the event. 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 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. Meredith Geary, CMP, Associate Director, NDIA
(703) 247-9476
mgeary@ndia.org
THANK YOU
FOR ATTENDING

We hope to see you at a future event!
View our Schedule of Events online:
http://www.ndia.org
The Economic Crisis and Its Impact on the DIB: Defense Industrial Base Forecasts 2010-2020

Presented By:

James H Averell
Economist
DCMA Industrial Analysis Center
james.averell@dcma.mil

27 April 2010
• BLUF
• Economic crisis history
• Current situation for DIB
  • Military Spending
  • NASA
  • Healthcare
• Economic forecasts and trends
• Additional DIB issues
• Final thoughts
### Demand
- Recession likely ended Summer 2009
- $1T stimulus for infrastructure, tax cuts, and healthcare reform
- $1.5T budget deficit for FY2010
- US reducing military effort in Iraq
- US surge in Afghanistan
- Healthcare reform
- Decline in Defense budget and contracting until 2020
- Investment and readiness compete for very scarce dollars against healthcare, entitlements, and economic recovery
- Aging DoD procurement workforce
- Aging and worn-out equipment

### Supply
- Recession hit the Defense and Aerospace industries in 2010
- Defense industry growth will be modest at best for next decade
- Defense industry likely to divest manufacturing capabilities
- Rising energy and raw material prices
- Labor Markets are contracting with a premium on skilled labor
- New round of Defense consolidation possible
- Increasing concentration of the DIB
- Increasing foreign ownership and dependency in lower tier industries
- Increasing spin-offs of manufacturing divisions
<table>
<thead>
<tr>
<th>Year</th>
<th>Events</th>
<th>Key Statistics</th>
</tr>
</thead>
</table>
| 2007 | •US and other housing market crash  
•Declining value of the U.S. dollar  
•Rising energy and materials costs  
•US economy falls into recession  
•Credit markets begin to freeze | •Estimated loses in real estate $150-$400B in the US  
•U.S. Gov’t deficit $162B (1% of GDP)  
•Fed funds at 4.5%  
•Manufacturing Capacity Utilization: 79% |
| 2008 | •Oil and Materials markets peak then crash  
•Major banks in the U.S. and Europe collapse  
•Global stock markets fall by 20-60%  
•Global coordinated reduction in interest rates  
•U.S./Fed implements $750 TARP and other bailouts | •Oil Peaks at $150/Barrel  
•S&P falls 45% between Jun-Nov  
•U.S. Gov’t deficit $455B (3.6% of GDP)  
•U.S. GDP falls 6.2% in real terms in 4th Qtr  
•Fed Funds rate falls to 0.25%  
•Manufacturing Capacity Utilization: 76% |
| 2009 | •Stock markets continue to decline  
•$787B American Reinvestment and Recovery Act (ARRA)  
•Consumers reducing debt and consumption spending  
•GM & Chrysler go bankrupt - $100B+ Bailout  
•Japanese, UK, & European economies in deep recession  
•Propose overhaul of financial regulation & U.S. healthcare | •DJI closes at 6594; 12yr low 2/2009  
•US Gov’t deficit: $1.8T (13% of GDP)  
•CPI declines first time since the 1950s  
•Unemployment hits 9.5%  
•Manufacturing Capacity Utilization at 65%  
•140 bank failures; highest since 1992 |
| 2010 | •Weak Recovery begins 2010 through stimulus spending  
•Big Banks have recovered; smaller banks still struggling  
•Sovereign Debt Crisis: | •US Govt Deficit $1.5T (9.8% of GDP)  
•Unemployment hits 10%  
•Manufacturing Capacity Utilization at 69.2%  
•50 additional bank failures |

Source: WSJ, BLS, OMB, CBO, Federal Reserve, & Value Line – 03/2010
Rising Tide Deficits and Debt

- Deficit around $1.4T for 2010 (10% of GDP)
- U.S. publicly held debt is projected to grow from 62% of GDP to 65%-82% range by 2020
- Rising government financing costs
- Falling tax revenue, rising unemployment, and healthcare costs
- Entitlement spending is projected to explode after 2018
- Growing global concerns on U.S. spending
- Healthcare reform: Historic Budget Buster?
- Bush Tax Cuts expire at the end of 2010: What tax cuts will be extended, if any?
- Japan now our largest creditor
- The $64 Trillion Question: How long are investors willing prop up the U.S. by buying U.S. Treasury Securities?

Source: Congressional Budget Office (CBO) 1/2010, WSJ, OMB, NDIA 3/2010, Tech America, & DCMA Analysis
# Healthcare Reform: Hope and Change

## Necessity
- Cost rising far faster than general inflation
- Rising amounts of chronic disease requiring continuing care
- Lack of IT penetration in this industry
- 45+ Million uninsured or under insured Americans
- Health issues leading cause of personal bankruptcy in the U.S.
- Reduces labor market efficiency and mobility
- US manufacturers are constrained by high health insurance costs
- Major factor in GM & Chryslers’ bankruptcies
- American manufacturers must compete against foreign companies that do not have to provide health insurance
- Forces more Automation – Substitution of Labor with Capital

## Costs and Provisions
- Affordability
- Cuts to Medicare by $500B
- Entitlement budget train wreck in 2018-2025
- Rising Medicare & other taxes
- No U.S. Tort Law reform
- Major provisions to date:
  - Full implementation in 2018
  - Requires most Americans and businesses to buy health insurance
  - Subsidizes for small business to provide health insurance to employees
  - Sets up Insurance exchanges
  - Heavily regulates health insurance providers
  - Taxes high end health insurance plans
  - Raise capital gains and taxes on incomes over 250K
  - Covers about 32M uninsured people

### Health Care: DIB Impact

<table>
<thead>
<tr>
<th>Impact on DoD &amp; DIB</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Potential squeeze on DoD spending after 2013</td>
</tr>
<tr>
<td>• Health reform could slow the growth of DoD healthcare programs (TRI-Care)</td>
</tr>
<tr>
<td>• Could keeps manufacturers in business – reduces cost burden</td>
</tr>
<tr>
<td>• Could reduce overhead costs for major prime contractors</td>
</tr>
<tr>
<td>• Allows for more responsive labor markets</td>
</tr>
<tr>
<td>• Improved healthcare access may keep aging population in the workforce longer</td>
</tr>
<tr>
<td>• Higher taxation levels could discourage economic growth</td>
</tr>
<tr>
<td>• Possible increase in administrative costs impacting overhead</td>
</tr>
<tr>
<td>• Large company write-downs impacting profitability</td>
</tr>
</tbody>
</table>
Sovereign Debt Crisis: Is US Next?

### Potential Next Steps

- Greece and European Nations are or near default on debt
- Currently the crisis is helping the US Dollar at the expense of the Euro
- Potential for new conflicts
- European Union debating a rescue package for Greece and other nations

### Sovereign Debt's Hot Spots

In light of the recent focus on sovereign risk and difficulties in the periphery of Europe, economists at RBC Capital Markets assembled a snapshot of economies to distinguish those that appear to be under the most duress. Among the several measures it examined were fiscal deficits, debt loads, growth rates and inflation. The ‘sovereign risk index’ included those and others. The higher the number the riskier the country. Click on column headers to sort the table.

<table>
<thead>
<tr>
<th>Developed Countries</th>
<th>Fiscal Balance (% of GDP)</th>
<th>Gross Public Debt (% of GDP)</th>
<th>Real GDP Growth %</th>
<th>Inflation</th>
<th>Sovereign Risk Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ireland</td>
<td>Much worse than average</td>
<td>Worse than average</td>
<td>Worst compared with average</td>
<td>Worst compared with average</td>
<td>0.90</td>
</tr>
<tr>
<td>Greece</td>
<td>Worse than average</td>
<td>Much worse than average</td>
<td>Much worse than average</td>
<td>Average</td>
<td>0.90</td>
</tr>
<tr>
<td>Portugal</td>
<td>Worse than average</td>
<td>Worse than average</td>
<td>Worse than average</td>
<td>Worse than average</td>
<td>0.59</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Much worse than average</td>
<td>Worse than average</td>
<td>Average</td>
<td>Average</td>
<td>0.52</td>
</tr>
<tr>
<td>Italy</td>
<td>Average</td>
<td>Much worse than average</td>
<td>Average</td>
<td>Average</td>
<td>0.43</td>
</tr>
<tr>
<td>France</td>
<td>Worse than average</td>
<td>Worse than average</td>
<td>Average</td>
<td>Average</td>
<td>0.37</td>
</tr>
<tr>
<td>Spain</td>
<td>Worse than average</td>
<td>Average</td>
<td>Much worse than average</td>
<td>Average</td>
<td>0.33</td>
</tr>
<tr>
<td>Japan</td>
<td>Worse than average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>0.28</td>
</tr>
<tr>
<td>United States</td>
<td>Much worse than average</td>
<td>Worse than average</td>
<td>Average</td>
<td>Average</td>
<td>0.21</td>
</tr>
<tr>
<td>Belgium</td>
<td>Average</td>
<td>Worse than average</td>
<td>Worse than average</td>
<td>Average</td>
<td>0.15</td>
</tr>
<tr>
<td>Austria</td>
<td>Average</td>
<td>Average</td>
<td>Worse than average</td>
<td>Average</td>
<td>0.14</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Worse than average</td>
<td>Average</td>
<td>Worse than average</td>
<td>Average</td>
<td>0.00</td>
</tr>
<tr>
<td>Germany</td>
<td>Average</td>
<td>Worse than average</td>
<td>Average</td>
<td>Average</td>
<td>-0.06</td>
</tr>
<tr>
<td>Canada</td>
<td>Average</td>
<td>Worse than average</td>
<td>Average</td>
<td>Average</td>
<td>-0.19</td>
</tr>
<tr>
<td>Finland</td>
<td>Average</td>
<td>Average</td>
<td>Worse than average</td>
<td>Average</td>
<td>-0.30</td>
</tr>
<tr>
<td>Denmark</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>-0.45</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>-0.49</td>
</tr>
<tr>
<td>Australia</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>-0.62</td>
</tr>
<tr>
<td>Sweden</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>-0.60</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Average</td>
<td>Worse than average</td>
<td>Worse than average</td>
<td>-1.06</td>
<td></td>
</tr>
<tr>
<td>Norway</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>-1.32</td>
</tr>
</tbody>
</table>

Source: Royal Bank of Canada Capital Markets
DoD Top Line Budget: 2000-2020

Source: TechAmerica 10/2009 & CBO 1/2010
Operations & Maintenance Budget

DoD Industry Addressable O&M Base Budget
Trends 2000-2020 Forecasts after 2010

Source: TechAmerica10/2009 & CBO 1/2010
DoD Contracting Trends

- Defense Industrial Base expands in terms of contracts and contractors because of the Global War on Terror
- As the wars wind down and the budget declines, the DIB will likely contract as contract awards fall
- The DIB expansion keyed by construction, consulting, and contracting out gov't. functions

# The QDR and Defense Budget Issues

<table>
<thead>
<tr>
<th>Quadrennial Defense Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>- First QDR to fully address wartime priorities</td>
</tr>
<tr>
<td>- Hybrid Warfare: prepare for conventional and unconventional war</td>
</tr>
<tr>
<td>- Need to take care of “Our People”</td>
</tr>
<tr>
<td>- Cyberspace domination</td>
</tr>
<tr>
<td>- Improve long range strike</td>
</tr>
<tr>
<td>- Shift to “Unmanned Systems and Capabilities” especially in aircraft</td>
</tr>
<tr>
<td>- New emphasis on cost and schedule over performance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Aging and Recapitalization Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Aging and war damaged platforms</td>
</tr>
<tr>
<td>- Many systems are at the end of design lifetimes</td>
</tr>
<tr>
<td>- Many vehicles are obsolete and worn out</td>
</tr>
<tr>
<td>- Can only reset and re-man a vehicle so many times</td>
</tr>
<tr>
<td>- High costs and delays in acquiring new systems</td>
</tr>
<tr>
<td>- About 85% of all Military vehicles need to be recapitalized or replaced</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defense Budget Cut?</th>
</tr>
</thead>
<tbody>
<tr>
<td>- High deficits and domestic priorities</td>
</tr>
<tr>
<td>- Decline in perceived threat</td>
</tr>
<tr>
<td>- Many high-tech systems are behind schedule and over budget</td>
</tr>
<tr>
<td>- Shifting emphasis from high-tech to proven low tech systems</td>
</tr>
<tr>
<td>- Potential Congressional push back</td>
</tr>
<tr>
<td>- On-going wars?</td>
</tr>
<tr>
<td>- Last War vs. the Next War?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perceived Weaknesses in Acquisition Workforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Too many cost overruns</td>
</tr>
<tr>
<td>- Hollowed out procurement DoD agencies:</td>
</tr>
<tr>
<td>- Increase of 20,000 acquisition workers</td>
</tr>
<tr>
<td>- DCMA declines from 30,000 in 1990 to under 10,000 in 2008</td>
</tr>
<tr>
<td>- DCMA to Hire 3,000?</td>
</tr>
<tr>
<td>- Reliance on contractor personnel</td>
</tr>
<tr>
<td>- Aging workforce in the Federal Government – average age is over 50 for most agencies</td>
</tr>
</tbody>
</table>

Source: DoD QDR 1/2010
### New Defense Build-up

- 20 Year Cycle going back to 1840s
- Entitlement issues will determine DoD’s budget
- New Technologies will require new systems
- 2020’s budget increases not likely to match 2000’s or the 1980’s
- Greater emphasis on investment accounts
- Unmanned Systems (Robotics) could reduce personnel requirements and costs
- Need to maintain near-term Science & Technology (S&T) investment to reduce long-term program risk

### Priority Programs

- Aging Inventories of aircraft, ships, and vehicles
- Aircraft: F-35, UAVs, Strategic Bomber, JTR, and Tankers/Air-lift
- Operationally Responsive Space (ORS) Systems
- Shipbuilding: CGX, DDGX, LCS, SSBNs, & Auxilliary Ships
- Combat Vehicles: JLTV, UGVs, Abrams, and Bradley replacements
- Missiles: Joint Common Missiles, Hypersonics, and Strategic Missiles
- Ammo & Weapons: New Infantry Rifle, Ammo, & Directed Energy
- Other: Chem/Bio Defense, Communications Gear & IT

### Questions

- Are we still in Iraq and Afghanistan?
- How will long-term budget issues be resolved?
- How well will current procurement programs for the 2010’s be funded?
- Peer Competitor vs. Irregular Warfare/Hybrid Warfare
- Can and will the US maintain global military capabilities?
- Will S&T investment be maintained?
- Controlling O&M costs
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• IT &amp; Digitalization</td>
<td>• Non-lethal Weapons</td>
</tr>
<tr>
<td>• Mult-Core Processing</td>
<td>• Directed Energy Weapons</td>
</tr>
<tr>
<td>• Terrahertz Computing</td>
<td>• Robotics</td>
</tr>
<tr>
<td>• Cloud Computing</td>
<td>• Unmanned Vehicles</td>
</tr>
<tr>
<td>• IT Security</td>
<td>• Loitering Munitions</td>
</tr>
<tr>
<td>• Nanotechnology</td>
<td>• Alternative Power Systems</td>
</tr>
<tr>
<td>• Carbon Nanotube Electronics</td>
<td>• Fuel Cell and Batteries</td>
</tr>
<tr>
<td>• Photon Electronics</td>
<td>• Solar Cells</td>
</tr>
<tr>
<td>• Motion Sensing &amp; Simulation</td>
<td>• Hypersonics</td>
</tr>
<tr>
<td>• Hull Coatings</td>
<td>• Kinetic Munitions</td>
</tr>
<tr>
<td>• Sensors - LADAR/LIDAR</td>
<td>• Advanced Propulsion – Scram Jet</td>
</tr>
<tr>
<td>• Sensors - LADAR/LIDAR</td>
<td>• Biotechnology</td>
</tr>
</tbody>
</table>
Non-Defense Discretionary Budget

Domestic Discretionary Budget Trends
2005-2020 Forecasts after 2009

Source: TechAmerica 10/2009
Civil Government rise driven by:

- ARRA investment
- Healthcare reform
- Replacement of retiring workers and automation of services
- IT Security is a top priority

Defense IT is basically stable

- Army IT declined in 2009 & 2010 as IT investment in support of Overseas Contingencies.
- IT investment need matches inflation over the next five years
- Continuing need to invest in the latest technology

Homeland Security Mission

Forecasts after 2010

$TRILION


- DHS - Discretionary Budget
- DHS - IT Budget
- Cross-Cutting - HLS Function in other Agencies
- Supplementals

Obama's Space Policy

- International Space Station (ISS) operates to 2020 and beyond
- Constellation cancelled as recommended by the Augustine Commission
- Focus on new technology development and launch facilities
- Shift in focus from established contractors to new start-ups
- Space contractors are assume greater amounts of program development and operational risk
- Obama’s budget adds $6B over the next 5 years
- Robust Planetary and Earth Observation program

Looming Gap with no U.S. Manned Space Vehicle available for 5+ years:

- NASA to retire the Shuttle in 2010/11
- No true Shuttle replacement vehicle possible before 2020
- Shift ISS supply and personnel ferrying missions to private sector contractors.
  - Space Ex – Falcon LV and Dragon Capsule are leading candidates
- Orion continues as a lifeboat for the ISS
- NASA's Man Rating requirements presents significant technical and cost challenges in developing manned space systems

Defense Budgets Peaked in 2008

- Aging equipment
- Interoperability with the U.S.
- Increasing international cooperation on defense programs: F-35 & MEADS
- Global Economic Crisis is reversing the trend

Defense spending is shifting from Europe to Asia

- Asian economies will have the money, population, and requirements
- Increasing security risks and threat perceptions in Asia

U.S. Exports are hampered because of the following:

- U.S. Systems are often too complex and costly
- Cheaper foreign alternatives
- Offset requirements
- U.S. Export controls are outdated

Crisis Impact on the DIB

**Falling Output & Rates of Capacity Utilization**
- Total manufacturing rate reached post WWII lows
- Hollowing out of US Industrial Base
- DIB utilization starting to decline
- China could overtake the U.S. in manufacturing by 2020

**Frozen Credit Markets**
- Small companies having difficulties securing financing for contracts
- Larger companies paying more for financing operations
- Little M&A activity except for small cash deals
- Increases in bankruptcies and liquidations

**High Unemployment**
- 10M+ jobs lost since Dec 2007
- Migration concerns
- Major Defense firms have started cutting jobs
- Delaying retirements and early retirement
- Rising unemployment and under-employment
- High cost of health insurance

Source: WSJ, Value Line, DCMA, Industrial Analysis Center, Federal Reserve, Census, & DCMA Financial Analysis Group
Commercial Aircraft Production Trends

**Boom times are at an end**
- Global Financial Market Meltdown in 2008
- Delays in deliveries
- Record low order intake in 2009
- Falling demand for business jets and general aviation aircraft
- Significant Supply Chain and Material Cost issues

**Shallower down-turn**
- Market expansion in the Middle East and Asia
- Aging aircraft, high fuel costs, and environmental concerns
- New models (787 & A350) from Boeing and Airbus to address above issues
- After declines in 2009, backlog still provides cushion

**Defense Industrial Base Impact**
- Workload stable for now but will likely decline in 2010
- Employment is likely to fall in 2010 but stable through 2016
- Concerns over sub-tier producers
- Rising overhead cost in the future

Source: Forecasts International 03/2010 & DCMA Analysis
## Defense & Aerospace Market Forecasts

<table>
<thead>
<tr>
<th>Forecast International Defined Aerospace and Defense Systems</th>
<th>Units</th>
<th>Value of Production in $2009M</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2010</td>
<td>2019</td>
</tr>
<tr>
<td><strong>Military Markets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Wing Military Aircraft</td>
<td>647</td>
<td>644</td>
</tr>
<tr>
<td>Military Helicopters</td>
<td>584</td>
<td>558</td>
</tr>
<tr>
<td>Launch Vehicles</td>
<td>40</td>
<td>22</td>
</tr>
<tr>
<td>Satellites</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td>Unmanned Systems</td>
<td>9,943</td>
<td>8,255</td>
</tr>
<tr>
<td>Aircraft Engines - Gas Turbines</td>
<td>3,052</td>
<td>1,650</td>
</tr>
<tr>
<td>Military Vehicles</td>
<td>31,395</td>
<td>9,565</td>
</tr>
<tr>
<td>Warships</td>
<td>24</td>
<td>27</td>
</tr>
<tr>
<td>Missiles</td>
<td>47,328</td>
<td>32,447</td>
</tr>
<tr>
<td>Munitions &amp; Weapons</td>
<td>652,100</td>
<td>457,461</td>
</tr>
<tr>
<td>Naval Systems</td>
<td>65,241</td>
<td>3,113</td>
</tr>
<tr>
<td><strong>Civil Markets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Wing Aircraft</td>
<td>3,520</td>
<td>5,794</td>
</tr>
<tr>
<td>Civil Helicopters</td>
<td>1,559</td>
<td>1,858</td>
</tr>
<tr>
<td>Aircraft Engines - Gas Turbines</td>
<td>8,024</td>
<td>10,555</td>
</tr>
<tr>
<td>Launch Vehicles</td>
<td>54</td>
<td>52</td>
</tr>
<tr>
<td>Satellites</td>
<td>66</td>
<td>18</td>
</tr>
<tr>
<td><strong>Combine Markets - Civil + Military</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Wing Aircraft</td>
<td>4,167</td>
<td>6,438</td>
</tr>
<tr>
<td>Helicopters</td>
<td>2,143</td>
<td>2,416</td>
</tr>
<tr>
<td>Aircraft Engines - Gas Turbines</td>
<td>8,064</td>
<td>10,577</td>
</tr>
<tr>
<td>Launch Vehicles</td>
<td>94</td>
<td>74</td>
</tr>
<tr>
<td>Satellites</td>
<td>81</td>
<td>23</td>
</tr>
</tbody>
</table>

Source: Forecast International 2/2010 - www.forecast1.com  Note: *CAGR - Compound Annual Growth Rate, **US% - US Based Producers Market Share
<table>
<thead>
<tr>
<th>Aging Workforce</th>
<th>Labor Migration</th>
<th>Foreign Sourcing and Ownership</th>
<th>Energy &amp; Material Costs and Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Crisis has delayed retirements and brought people back to the workforce</td>
<td>• To contain costs, manufacturing work is shifting out of the Midwest, Northeast, and Pacific States to interior South and Southwestern states</td>
<td>• Falling dollar encourages foreign sourcing and mergers with foreign partners</td>
<td>• Plunge in oil prices</td>
</tr>
<tr>
<td>• Highly skilled workers will be in short supply, especially, engineers, scientists, and computer personnel</td>
<td>• Many Aircraft and Spacecraft production facilities are over 50 years old</td>
<td>• US DIB is being hollowed out by foreign dependencies for key components</td>
<td>• Inflation could return</td>
</tr>
<tr>
<td>• Traditional “Defined Benefit” retirement programs are being replaced by 401K “Defined Contribution” programs</td>
<td>• Differences in cost of living and taxation driving worker and company migration trends.</td>
<td>• Industrial “Know How” is moving overseas</td>
<td>• Reduction in mining capacity and slowing of the growth of energy production</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Infrastructure, healthcare issues, lack of skills, tax climate, and regulations hinder competitiveness</td>
<td>• China and India are still growing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Current recession slowing the growth of energy &amp; mining productive capacity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ARRA has money for Alternative Energy development</td>
</tr>
</tbody>
</table>
### U.S. Defense Consolidation Outlook

#### Thawing merger & acquisition market
- Frozen credit markets in 2008 are now beginning to thaw
- Budget uncertainty created by QDR and lack of guidance from DoD
- Budget cuts could spur a new round of consolidation in the next decade
- Private Equity Investment companies could dump defense companies

#### Technology & Policy Change Creates Growth
- Growth of UAV's will bring Aircraft players into the market
- Operationally Responsive Space (ORS) allows for Small Satellites and Launch Vehicle use by DoD
- Foreign competition and penetration in US DIB is possible

#### Manufacturing facility consolidation
- Prime contractors focusing on design, integration, and service providing at the expense of manufacturing
- Aging facilities with aging workforces in high cost geographical areas
- Need to maximize shareholder value
- Supply chain issues could mitigate this trend
## Final Thoughts

### Points to Ponder

- Recession is likely over but the recovery is weak
- Administration fiscal policy along with monetary policy is extremely expansive and will have significant long-term impact on the economy
  - Stimulus in 2009
  - Healthcare Reform
- Defense top line is going to take cuts: How Much and When?
- The QDR repeats many policies and goals expressed over the past 20 years
  - New Urgency on cost containment and schedule
  - Preparation for a multiple types of warfare
  - Emphasis on IT and Cyberwarfare
- DIB is in good shape to weather this down-turn
National Infrastructure Protection Plan (NIPP) Partnership Model and Cross Sector Cyber Security Working Group (CSCSWG)

DIB CIP Conference, 27 April 2010

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

- NIPP Federal Senior Leadership Council (FSLC)
- Critical Infrastructure Protection Advisory Council Framework
- Partnership for Critical Infrastructure Security
- National Council of ISACs
- Other Ad-Hoc Groups as needed
- US-CERT
- Software Assurance Forum
The National Guard Bureau
Critical Infrastructure Program in
Conjunction with the Joint Interagency
Training and Education Center

Brigadier General James A. Hoyer
Director Joint Staff
West Virginia National Guard

and

Colonel Thomas McGinley
Provost Marshal J34
National Guard Bureau

This briefing is
UNCLASSIFIED

As of 23 APR 2010
Authorities

- Homeland Security Presidential Directive-7 (HSPD-7)  
  - December 17, 2003

- Defense Critical Infrastructure Program (DCIP), (DoDD 3020.40)  
  - January 14, 2010

- National Infrastructure Protection Plan (NIPP)  
  - June 2009
National Guard CIP-MAA Teams

- Critical Infrastructure Protection- Mission Assurance Assessment (CIP-MAA) Teams conduct assessments in support of the DoD Defense Industrial Base (DIB)
  - All-hazard, vulnerability assessments of DIB sites deemed critical by Assistant Secretary of Defense (HD/ASA)
  - Teams are composed of 9 National Guard Soldiers and Airmen
  - Standardized report allows Defense Contract Management Agency (DCMA) to build a common operational picture for risk management decisions
  - Historical data will allow DCMA to begin trend analysis

**Desired Effect:** DoD executes wartime missions regardless of man-made or natural hazards to critical DIB sites
• 6 Assessment teams initially developed

• Concept was validated by Joint Requirements Oversight Council (JROCM 29 Jan 07)

• 3 Teams fielded to support Defense Industrial Base (DIB) mission
NG CIP-MAA Team Composition

- 3 Nine-Person CIP-MAA Teams authorized to support the Defense Critical Infrastructure Program

- Teams are Comprised of:
  - Team Leader
  - Mission Analyst
  - Electric Power Analyst
  - Transportation Analyst
  - Communications Analyst
  - HVAC Analyst
  - Natural Gas and Petroleum Analyst
  - Chemical and Water Analyst
  - Security and Emergency Management Specialist
NG CIP-MAA Team Training

- Team members receive:
  - Defense Critical Infrastructure Protection Assessment Methodology Training
    - Mission Assurance based training
    - Phase I - 5 Days classroom training
    - Phase II - On-the-Job training assessment
  - JITEC - Enhanced Comprehensive Assessment Model Training
    - Antiterrorism / Force Protection based training with an all-hazards approach
    - 5 Days classroom instruction and a 5 day mock assessment
NG DHS CIP Teams

- Department of Homeland Security Critical Infrastructure Protection Assessment (DHS CIP) Teams
  - Teams are composed of 3 NG Soldiers and Airmen
  - All-hazard, vulnerability assessments of critical DHS sites
  - Standardized reports will allow DHS to build a common operational picture for risk management decisions
  - These teams differ from CIP-MAA teams due to training and assessment requirements
  - 1 Three-Man Standard Evaluation Assessment Team (SEAT) for the evaluation of NG DHS CIP teams and assessment execution

**Desired Effect:** Enables DHS to refine threat mitigation strategies of sites, critical to the United States
• 19 teams selected to support DHS
• 18 teams trained
• 1 team currently completing member selection
• At least 1 team per FEMA region
QUESTIONS?
Defense Critical Infrastructure Programs (DCIP)  
Mission Assurance Assessment

• Presented By:
Steve Turdo – DCMA Industrial Analysis Center  
Maj Scott White – NY National Guard  
2Lt Jeremy Samples – WV National Guard  
1SG Jon Huddleston – CO National Guard

• February 2010
Outline

- DCMA Planning
- Advance Visit – Mission Analyst
- Supporting Foundational Infrastructure Analyst Duties
- MAA Report process
- 12 Month follow up
DCMA Planning

• Initial Company Contact
• IAC Industrial Capabilities Assessment
• Letter of Intent to Company
• MOA between IAC and Company
• Number of contacts / visits prior to assessment
• Security Operations & Emergency Management
• National Guard Teams
• Lessons learned
Pre Assessment
The Team

- DCMA Responsibilities
- Team Construct
- Team Leader Responsibilities
- Mission Analyst Responsibilities
- SFIN Responsibilities
• Understanding the Mission
• Interacting with the Company
• Interacting with DCMA
  • IAC
  • CMO
• Developing the Mission Map
Mission Focused Assessment Summary

- **DCMA**
- **Mission Focus**
- **Mission Functions**
- **Supporting Tasks**
- **Asset Identification/Characterization**
- **Infrastructure Asset Dependency Identification/Characterization**

- **Vulnerability Analysis**
- **Threat**

- **Mission Impact Analysis**
- **Risk**

- Identified Pre-Assessment
- Preliminary Identification Pre-Assessment/Finalized Identification and Characterization On Site
- Performed On Site as Possible; Completed Post-Assessment
Assessment
Assessment

- In Brief / Meet and Greet
- Mission Focus Production Tour
- Production Infrastructure Dependencies Tour
- Interviews / Data Collection
- Daily Hot Washes
- Mission Focus Mission Map Finalization
- Supporting Foundational Infrastructure Network Mission Map Development
- Mission Impact Analysis
Mission Impact Analysis
Post Assessment
CIP – MAA Report Process

- Out brief (in process review)
- Steps upon return
- Contacting site for additional information
- Length of Report & Report writing for each section
- Final Product
- DCMA submission & review
Path Forward

- Refine report writing tool
- CIP-MAA team Conference
- Regional Resiliency Assessment Program (RRAP)
- Develop FY11 assessment schedule
  - By APM ranking
  - Continue to assess weapons platforms
  - DIB geographic concentration
Questions?

Thank You
Panel Discussion
DIB Sector Involvement in Recent & Planned Exercises

Panel Moderator:
Colonel Paul T. Ahern, USAR
Director, Joint Reserve Response Team
Homeland Defense Operations Division
DCMA – Industrial Analysis Center (IAC)

Wednesday, April 28, 2010
• **Panel Members:**

  • **Mr. John Schauffert**, Assessments Branch Chief, Force Protection & Mission Assurance Division, U.S. Northern Command J-34

  • **Ms. Nancy Pomerleau**, Executive Director, Partnership & Outreach Division, Department of Homeland Security Infrastructure Protection

  • **Mr. David Kemeter**, DIB Preparedness Program Manager, Defense Contract Management Agency, Industrial Analysis Center Homeland Defense Operations Division

  • **Mr. Robert Connors**, Preparedness Director, Raytheon Company
• DCMA Industrial Analysis Center:
  
  • **FY 09 – Exercise Involvement**
    • IAC Homeland Defense Operations Division - Annual Preparedness Exercise
    • US NORTHCOM - Ardent Sentry Exercise
    • DHS – National Level Exercise 2009
    • BAE Greenlawn, NY (Suffolk County) – TTX
  
  • **FY 10 & 11 – Exercise Involvement**
    • US NORTHCOM – Vigilant Shield 10
    • IAC-HDAT - Small Exercise IAC-09-001 (JRT)
    • US Army War College – Strategic Decision Making Exercise
    • DHS - National Level Exercise 2010
    • IAC Homeland Defense Operations Division – Annual Preparedness Exercise
    • US NORTHCOM – Ardent Sentry
    • US NORTHCOM Vigilant Shield 11
    • DHS - National Level Exercise 2011
• DCMA Industrial Analysis Center:

• **DIB Sector: Tiered Reserve Force Augmentation Plan**

  • Tier 1 – IAC Homeland Defense Operations Division Civilian Workforce
  
  • Tier 2 - Navy Reservists
  
  • Tier 3 - Army Reservists
  
  • Tier 4 – TBD
USTRANSCOM
Critical Infrastructure Program
(CIP)

28 April, 2010
Jake Carson, CIP Branch Chief
TCJ3-FC

wayne.carson@ustranscom.mil
(618) 256-4446
DCIP Roles and Responsibilities (Cont)
National Program – Consequence focused

- Critical Infrastructure Protection (CIP)
- Critical Infrastructure / Key Resources (CI/KR)
  - Loss of life
  - Economic Impact

DOD Program – Mission focused

- Defense Critical Infrastructure Program (DCIP)
- Defense Critical Infrastructure/Asset (DCI)/(DCA)
  - Mission Failure or Degradation
    - Specific Mission Essential tasks by identified Operation Plans
  - Function Failure or Degradation
    - Move Cargo, Move Passengers, Move Patients, and Provide C4
  - Essential to Mission Assurance
DCIP Roles and Responsibilities (Cont)

TCJ3 is "CIAO"

*** Critical Infrastructure Assurance Officer

DEFENSE SECTORS, LEAD AGENCIES & PRINCIPAL STAFF ASSISTANTS

Transportation USTRANSCOM
Public works USACE
Logistics DLA
DIB DCMA
Financial Services DFAS
Health Affairs ASD(HA)
Personnel DHRA
GIG/C2 DISA
ISR DIA
Space USSTRATCOM

USD(Policy)

ASD(HD&ASA)
Director, CIP
CIP Oversight & Resource Advocate

USD(AT&L)

USD(C)

USD(P&R)

USD(I)

ASD(NII)

ASD(ISP)

JOINT STAFF

MILITARY DEPARTMENTS
Operations Advisory Board (OAB)

SERVICES/NGB

COMBATANT COMMANDS

Defense Agencies

Defense Field Activities

Secretary of Defense

• Governance Council
• Critical Infrastructure Protection Integration Staff (CIPIS)
• Defense Infrastructure Sector Council (DISC)

USTRANSCOM Responsibility for a
Transportation Defense Sector CIP

DODD 3020.40

USTRANSCOM Responsibility for a
Combatant Command CIP

*** Critical Infrastructure Assurance Officer
Applying CIP to the Transportation Mission

USTRANSCOM Responsibility for a Transportation Defense Sector CIP

The Transportation Defense Infrastructure Sector DCI (DOD, Non-DOD, and foreign owned critical assets)

USTRANSCOM DCI (DOD owned Transportation critical assets)

Foreign Owned Transportation Sector DCI

USTRANSCOM Responsibility for a Combatant Command CIP
The DCIP Risk Management Process

Risk Management Decision
- Accept Risk, or
- Reduce Risk to Acceptable Level

Risk Response
- Implement Decision
  - To Accept Risk
  - To Remediate
  - To Mitigate
  - To Restore

Decompose
- Missions
- Functions

Risk Assessment
- Identify DCI
- Identify Threats & Hazards to DCI
- Assess DCI Vulnerabilities

Assess Risk
- Determine Consequence of Loss
- Evaluate Importance and Urgency of Action
- Develop Alternative Courses of Action

Monitor Implementation of Risk Management Decision

Monitor Threat & Hazard Changes

Post Progress and Status
Applying CIP to the Transportation Mission (Cont)

• Mission Decomposition to Identify DCI
  - Deploy, Redeploy, Sustain, Patient Movement, Command and Control, and Intelligence
  - Identify Standards, conditions and capabilities required for specific Transportation Missions and Functions

• Identification/Analysis of DCI
  - DOD military installations
  - Commercial seaports/airports
  - Commercial rail lines/yards
  - State/local roadways
  - Waterways

TAKEAWAY:
DOD, Federal, Public, and Private industry owned and/or operated infrastructure focus

• Identification of Threats and Hazards to DCI
• Identification of Vulnerabilities to DCI
• Identification of Dependencies to DCI
• Risk Management Decision for DCI
• Monitoring/Reporting Status of DCI
Identification of Dependencies to DCI

- Dependecy analysis of TCAs
  - Electricity
  - Fuel
  - Bridges
  - Waterways
  - Etc

- Joint Staff issues the DCIP TCA list
- Transportation Sector responsibility
Identification of Threats and Hazards to DCI

- All hazards approach (natural and manmade)
- Defense Intelligence Agency, TCJ2, Federal Bureau of Investigation, Department of Homeland Security, State/local police, etc
- Combatant Commands, Military Services, and Intelligence offices
- Enhanced Threats and Hazards Assessment
Identification of Vulnerabilities to DCI

Current Program

- Provide **Transportation Infrastructure Subject Matter Expertise** for DCIP Assessments with a Transportation mission focus

- Exploring **partnership opportunities** with other government agencies (DHS, TSA, USCG, etc.) at non-DOD owned locations:
  - Commercial Seaports
  - Commercial Airports
  - Interstate Highway Network
  - Rail Network

*VULNERABILITY* ... could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

* DODD 3020.40
The DCIP Risk Management Decision

- Accept the risk
- Remediate the risk
- Mitigate the risk
- Reconstitute the asset

Reduce risk to an acceptable level from threat, hazard, or vulnerability

DCIP GOAL: Reduce or eliminate unacceptable risk to DCAs, thus enabling the successful execution of DOD missions, regardless of the threat or hazard.
Questions...

...Our Focus is to Support the Warfighter
The Company - Five Operating Sectors

Aerospace Systems
Large Scale Systems Integration
C4ISR
Unmanned Systems
Airborne Ground Surveillance / C2
Naval BMC2
Global / Theater Strike Systems
Electronic Combat Operations
ISR Satellite Systems
Missile Defense Satellite Systems
MILSATCOM Systems
Environmental & Space Science Satellite Systems
Directed Energy Systems
Strategic Space Systems

Electronic Systems
Radar Systems
C4ISR
Electronic Warfare
Naval & Marine Systems
Navigation & Guidance
Military Space
Government Systems

Information Systems
Command & Control Systems
Network Communications
Intelligence, Surveillance & Reconnaissance Systems
Enterprise Systems and Security
IT/Network Outsourcing
Intelligence
Federal, State/Local & Commercial
Homeland Security & Health

Shipbuilding
Naval Systems Integrator
Surface Combatants
Expeditionary Warfare Ships
Auxiliary Ships
Marine Composite Technology
Coast Guard Cutters
Commercial Ships
Nuclear Aircraft Carriers
Nuclear Submarines
Fleet Maintenance
Aircraft Carrier Overhaul & Refueling

Technical Services
Systems Support
Base and Infrastructure Support
Range Operations
Maintenance Support
Training and Simulations
Technical and Operational Support
Live, Virtual and Constructive Domains
Life Cycle Optimization
Performance Based Logistics
Modifications, Repair and Overhaul (MRO)
Supply Chain Management
Lead Support Integrator (LSI)
Corporate Contingency Planning

- Five Varied Product Operations but a Consolidated Security Focus

- Corporate Policy J1 “Security” – Seven Major Processes
  - Personnel Security
  - Information Security
  - Physical Security
  - Investigations
  - Fire Protection
  - Contingency Planning
  - Security Quality and Oversight

- This is the Common Charter for Security Activity in Every Sector

- Corporate Security Functions Under Enterprise Shared Services. Was Under HR Until Recently; Remains Under HR at Sectors
Corporate Contingency Planning

• Corporate Procedure – “Business Continuity Program”
  - Sub-Procedure – “Definitions” Ensures Common Terminology
  - Sub-Procedure – “Business Continuity Program Guidelines” Provides Planning Outlines and Defines Required Content

• Corporate Procedures are Supplemented and Tailored by Sectors to Address Unique Business Aspects and Issues… BUT

• A Standard Business Continuity Program (BCP) Paradigm Applies at All Company Elements
Definitions Focus Operational Philosophy

• Crisis: “Any unplanned event or situation, including human-caused events and natural disasters, which threatens, or has the potential, to adversely affect the business area/site as a whole in terms of its existence, reputation, values and beliefs, systems, finances, physical plant, or the medical, environmental, and emotional well being of persons within and around the facility.”

• Crisis Management: “A top-down, coordinated approach to provide leadership, decide policy, and direct actions to prepare for, prevent, and respond to incidents that escalate beyond the business area/site’s normal response capability.”

• Critical Process: “Business processes which, if significantly disrupted, would have an adverse impact on the company’s personnel, operations, revenue, customer schedules, contractual commitments, or legal obligations.”
Corporate Contingency Planning

SITE EMERGENCY RESPONSE PLAN (Linked to HAZMAT and Fire Prevention Plans)
- Escalated Response
- Communications
- Personnel Accountability
- Personnel Evacuation
- Emergency Response
- Employee Education

FOCUS: PEOPLE
- OSHA Requirements

SITE CRISIS MANAGEMENT PLAN
- Transition to Business Contingency Team
- Initial Assessment
- Incident Containment
- Responsibilities Notifications Activation

FOCUS: DECISION PROCESSES

SITE AND/OR FUNCTION/ IPT BUSINESS RESUMPTION PLANS
- Process Contingency Plans (FOR CRITICAL PROCESSES)
- Recovery Strategies Approved by Management
- Critical Process Identification
- Management Guidance & Analysis

FOCUS: BUSINESS REVENUE
- Escalated Response

BUSINESS IMPACT ANALYSIS

RISK ASSESSMENT & VULNERABILITIES ANALYSIS

CORPORATE AND SECTOR REQUIREMENTS

VITAL RECORDS PROGRAM

INFORMATION SYSTEMS, TELECOMMUNICATIONS, AND FACILITIES

EXECUTIVE PROTECTION
Corporate Contingency Planning

• The Wide Variety of Potential Emergencies and Business Crises

<table>
<thead>
<tr>
<th>Types</th>
<th>Natural</th>
<th>Human</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical emergency</td>
<td>Fire (internal and external)</td>
<td>Power interruption</td>
<td>Flood</td>
</tr>
<tr>
<td>Bomb threat</td>
<td>High winds (radar range)</td>
<td>Snow storm/Blizzard</td>
<td>Aircraft crash</td>
</tr>
<tr>
<td>Hurricane</td>
<td>Hurricane</td>
<td>Earthquake</td>
<td>Workplace violence</td>
</tr>
<tr>
<td>HAZMAT spill</td>
<td>Outdoor winds (radar range)</td>
<td>Tornado</td>
<td>Product quality defect allegations</td>
</tr>
<tr>
<td>Civil disorder</td>
<td>High winds (radar range)</td>
<td>Workplace violence</td>
<td>Network penetration/exfiltration</td>
</tr>
<tr>
<td>Terrorist threat/Attacks</td>
<td>Outdoor winds (radar range)</td>
<td>Outdoor winds (radar range)</td>
<td>Insider threat</td>
</tr>
<tr>
<td>Explosion</td>
<td>Outdoor winds (radar range)</td>
<td>Outdoor winds (radar range)</td>
<td>Pandemic</td>
</tr>
<tr>
<td>Law Enforcement actions (raids)</td>
<td>Outdoor winds (radar range)</td>
<td>Outdoor winds (radar range)</td>
<td>Pandemic</td>
</tr>
<tr>
<td>Product sabotage</td>
<td>Outdoor winds (radar range)</td>
<td>Outdoor winds (radar range)</td>
<td>Pandemic</td>
</tr>
<tr>
<td>Denial of Service cyber attacks</td>
<td>Outdoor winds (radar range)</td>
<td>Outdoor winds (radar range)</td>
<td>Pandemic</td>
</tr>
<tr>
<td>Intellectual property loss</td>
<td>Outdoor winds (radar range)</td>
<td>Outdoor winds (radar range)</td>
<td>Pandemic</td>
</tr>
</tbody>
</table>

Scale and Impact Define Problem & Response
Corporate Contingency Planning

- Enterprise BCP Requires Three Plans be Established, Implemented, Tested and Updated at Least Annually at Every Facility:
  - Emergency Action Plan (EAP)* – What employees are to do in an emergency (Evacuation, Accountability, Recovery, Communication)
  - Crisis Management Plan (CMP)* – How management structures and reacts to deal with any of the multiple types of major or more enduring crises that can occur (CM Team is Defined and Roles Established; CM Room Established; Equipment Pre-Positioned; Checklists Developed for Various Types of Crisis)
  - Business Resumption Plan (BRP)** – How senior management returns things to normal (BR Team Defined and Roles Established; Tasks and Checklists Pre-Determined)

* Security has management responsibility
** Senior business executive has responsibility to restore business activity
Priority is on Rapid Disaster Recovery – Physical and Cyber

- **Emergency Response:** Survive and Terminate
  - React to the issue
  - Care for the people
  - Restore reasonable normalcy ASAP
- **Crisis Management:** Evaluate the New Reality
  - Marshal your resources according to plan
  - Gather data and evaluate the situation
  - Organize to address changed conditions
  - Mitigate collateral fallout
- **Business Resumption:**
  - Evaluate losses and quantify restoration needs
  - Tailor the plan from general to specific, test and refine it
  - Execute the plan; get back to business
Corporate Contingency Planning

- Heavy Focus on IT Security and Systems Recovery
  - All Info Systems are Subject to Business Impact Analysis (BIA) – “A documented product that assesses the value and impact of loss or delay in execution of the critical system(s) identified by functions.”
  - Critical Systems, Determined by BIA, Require an Information System Continuity Plan (ISCP) – “Sets forth the planning actions, procedures, and responsibilities necessary for the short- and long-term restoration of information systems supporting critical business operations.”
  - Test Plans are Required and Exercised for Each ISCP
  - Risk, in Lieu of ISCP, May be Accepted by Users for Less Critical Systems – But Users Must Document Their Justification for Risk Acceptance

Businesses Cannot Function Without IT
Corporate Contingency Planning

• Pandemic Preparedness – A Planning Case Study
  – Early 2006 – Corporate cadre began outlining a plan to address a potential Bird Flu (H5N1) pandemic, to address and mitigate business impacts
  – Earlier SARS concerns, and the predicted inevitability of human-to-human H5N1 infection at some point, dictated the wisdom of advance planning
  – Worldwide situation is already in Phase 3, per United Nations definition

• Pandemic Sub-Team Formed Under Hq Crisis Management Team:
  – Corporate Functions Participating: Environmental, Health & Safety, HR, Security (Chair), Travel, Law, Risk Management, Finance, Benefits, Corporate Communications, Global Supply Chain
  – Team decided advance executive planning was needed to address:
    • Medical/medication practices; Pay policy; Travel restrictions; Evacuation policies; Alternate work locations; Remote access capabilities; Alternate workforce; Quarantine & isolation policy; Allowable & mandatory time off; Return to work process; Coverage for local government lapses

Specific Proactive Planning
Corporate Contingency Planning

- Pandemic Preparedness – A Planning Case Study (continued)
  - Key communications: Employee awareness – potential threat; general prevention measures; preventive measures to take during Phases 4 – 6
  - Identify essential employees and essential suppliers

- Planning Approach – Outline Company Actions Progressively from Phase 3 (current) Through to Full Phase 6 Pandemic
  - Basic Corporate Plan published in May 2006 with functional enclosures outlining specific tasks, by phase
  - Plan supplements were required from all business sectors
  - We continue to monitor Bird Flu status worldwide

- 2009 Swine Flu (H1N1) Experience Has Refined the Planning Model
  - Relative virulence of a strain is recognized as a more significant factor than simple widespread prevalence, even at Phase 6
Corporate Contingency Planning

• The Ultimate Crisis – Hurricane Katrina – A Case Study

• Eight Company Locations Were Impacted in 2005

• Corporate and Cross-Functional Multi-Sector CMTs Acted
  – Assessed Needs and Coordinated Efforts to Deliver Essential Provisions:
    • Food, ice, water, fuel, vehicles, trailers, generators, forklifts, communication capabilities, payroll, physical security.
Corporate Contingency Planning

• Katrina Recovery

• Business Resilience Benefited from Having the BCP Structure in Place, from Advance Planning and applying a Flexible Focus
  - Swift and efficient action prevented worse business disruption and expedited the return to normal.
  - Within three weeks, power was restored at Ship System facilities and over 10,000 employees were back to work.
    • Remember, Katrina had impacted employee homes, families and lives.
  - Within five weeks, 12,500 employees back to work.
  - Resilience = Rapid Recovery: Benefits both customers and the company.

• Lessons Learned Were Documented – Information Shared
  - Corporate CMT began compiling experience data within 30 days of event.
  - Document shared with CMTs company-wide within 60 days after the event.
Corporate Contingency Planning

• A BCP Strategy of Partnering with Neighbors Builds Relationships

• Relationships Establish Trust and Pay Dividends

• Example:
  - NGC Corporate Hq Security partnered to develop the Century City Mutual Aid Structure
    • Focus on earthquake, fire, terrorism, civil disorder, crime
  - Worked with Los Angeles PD, Sheriff, Fire, and other Century City businesses, large and small
  - NGC hosted meetings (donuts can draw participation and make friends)
  - Helped draft and coordinate planning documentation
  - Crisis Management Teams and Control Center locations pre-planned
  - Participants and roles defined; contact lists developed
Corporate Contingency Planning

• The Future Focus – Prepare for and Prevent Major Cyber Crisis
  – Current mitigating actions
    • Consolidate corporate data centers (4) – Better control and organization
    • Decentralize locations – Spread the risk around the compass
  – Cyber Security Operations Center – A Benchmark Operation
    • 24/7/365 security monitoring of networks, servers and desktops
    • Computer security incident response and investigations provides containment, analysis and restoration
    • Digital forensics expertise
  – Cyber Threat Analysis and Intelligence Team (CTA&I)
    • Expertise: East Asia/China military intelligence, information warfare, advanced hacking, malicious systems and software, network security
    • Mission: Identify and stop the Advanced Persistent Threat (APT)
QUESTIONS?
Training and Exercises

Homeland Security Exercise and Evaluation Program
http://www.hseep.dhs.gov

FEMA Lessons Learned Information Sharing
http://www.llis.gov

FEMA Emergency Management Institute
http://training.fema.gov/IS/crslist.asp

Business
http://www.dhs.gov/xbsnss/

Critical Infrastructure Protection
http://www.dhs.gov/files/programs/critical.shtm
Al-Qa’ida and Affiliates—Homeland Plotting

- Al-Qa’ida, its affiliates and allies, remain dangerous and adaptive enemies:
  - We lack *insights into specific details, timing and intended targets* but assess al-Qa’ida continues to pursue plans for Homeland attacks.
  - Historically AQ focused on prominent *political, economic and infrastructure targets* to produce mass casualties, visually *dramatic destruction, significant economic* aftershocks and fear among the population.
  - However, recent events suggest possible trend in which terrorists seek to conduct small, easy attacks.

Sources: 2007 National Intelligence Estimate: Terrorist Threat to the Homeland
DNI Annual Threat Assessment-February 2009
Media Statements Highlight Call for Action

- March 17 statement by Yemen-based Anwar al-Aulaqi continues recent calls for attacks upon civilians and infrastructure within the United States by extremist ideologues.¹

- On March 7, al-Qa’ida media spokesman Adam Gadahn called for additional attacks similar to those executed and attempted by Ft. Hood suspect Maj. Nidal Hasan and accused Christmas Day bomber Umar Farouk Abdulmutallab
  - “…unsuccessful attacks on Western mass transportation systems can bring major cities to a halt, cost the enemy billions and send… corporations into bankruptcy.”²

- In January Usama bin Ladin repeated his criticism of the U.S. and its policies in a video statement,
  - He instructed individuals within the U.S. to hold large corporations and politicians accountable for economic downturn.³

² NEFA Foundation, http://www.nefafoundation.org
Homeland Threat Environment

- Recent attacks, arrests and plot disruptions indicate a continued violent extremist threat to the Homeland.
  - Arrests of US-based al-Qa’ida associates last year suggest the organization has succeeded in positioning Homeland-focused operatives in the U.S.
  - Ties that the Christmas Day attacker had to AQ affiliate al-Qa’ida in the Arabian Peninsula represent new Homeland threat concerns
  - Somali-Americans continue to show interest in returning to East Africa to participate in the ongoing conflict in Somalia
  - Separately, U.S.-based violent extremists with no overseas connections generally have the intent to conduct an attack but lack capabilities of those connected to terrorists overseas.
Important Arrests in the US

- Arrests of Zazi and his associates indicate overseas terrorist groups had operatives in the U.S. capable of facilitating and carrying out attacks.

  — Zazi was allegedly in direct operational contact with an al-Qa’ida associate in Pakistan and plotting against targets in the U.S.
  — Zazi allegedly planned attacks against the NYC subway system\(^1\)
  — Zazi and co-conspirators Adis Medunjanin and Zarein Ahmedzay received training in Pakistan to include the use of explosives\(^2\)

---

\(^1\) Department of Justice, Office of Public Affairs, Monday, February 22, 2010 Najibullah Zazi Pleads Guilty to Conspiracy to Use Explosives Against Persons or Property in U.S., Conspiracy to Murder Abroad and Providing Material Support to Al-Qaeda

\(^2\) Department of Justice Office of Public Affairs, Thursday, February 25, 2010 Two Charged with Terror Violations in Connection with New York Subway Plot
Important Arrests in the U.S.

- Chicago man was arrested and charged with allegedly planning attacks against Denmark and India

  — Charges against David Headley, who pleaded guilty last week, stem from his support to the Mumbai attacks, including facilitation of pre-attack planning and surveillance.

  — Headley charges included conducting surveillance of newspaper offices in Denmark in support of possible terrorist attacks there.

  — Charges highlight the al-Qa‘ida links to the planned attack in Denmark and explain the significant involvement of Ilyas Kashmiri, a prominent Pakistan-based terrorist with ties to al-Qa‘ida

1 DOJ Press Release and Indictment dated Thursday, March 18, 2010 CHICAGO RESIDENT DAVID COLEMAN HEADLEY PLEADS GUILTY TO ROLE IN INDIA AND DENMARK TERRORISM CONSPIRACIES Admits Conducting Surveillance for Lashkar e Tayyiba in Planning 2008 Mumbai Attacks Indictment
Dec. 25, 2009, Attempted Aviation Attack

- Al-Qa’ida regional affiliate AQAP, which has advocated attacks on the U.S. Homeland in the past, directed Umar Farouk Abdulmutallab and provided him training and explosives.\(^1\)

- Lessons learned are still emerging; however, initial observations:
  - Compressed planning cycle\(^2\)
  - Artful concealment\(^3\)

- We are still exploring what other Homeland plots AQAP and associated Yemeni extremists may have planned. We are concerned that they will continue to try to do so.\(^1\)

---

\(^1\) Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence
\(^2\) 2 February 2010
\(^3\) LA Times, Al Qaeda’s New Tactic is to Seize Shortcuts
\(^3\) DHS-FBI Joint Roll Call Release, 29 December 2009
Somali Diaspora Support to al-Shabaab

- We judge most Al-Shabaab and East Africa-based al-Qa’ida members will remain focused on regional objectives in the near-term.
- East Africa-based al-Qa’ida leaders or al-Shabaab may elect to redirect to the Homeland some of the Westerners, including North Americans, now training and fighting in Somalia.
- Somali-Americans playing larger role in conflict; individuals leading attacks and conducting suicide bombings.¹
- An American from Houston was charged with receiving terrorist training from al Qa’ida; others from Minneapolis have also been charged with similar counts.²

¹ Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence 2 February 2010
² Department of Justice Press Release For Immediate Release November 23, 2009United States Attorney's Office District of Minnesota Terror Charges Unsealed in Minnesota Against Eight Defendants, Justice Department Announces
Autonomous Violent Extremists

- Arrests last summer illustrate the threat posed by U.S.-based extremists
- These individuals are more reliant on additional participants

— Hosam Smadi in Texas, Michael Curtiss Finton in Illinois and James Cromitie in New York asked law enforcement informants to obtain weapons and explosives
— Tarek Mehanna considered attacking malls a few years ago but claimed he was unable to do so because he could not gain access to automatic weapons

Implications: These individuals identified with the ideas and goals of the global jihadist movement, but lacked direct guidance or instructions from the leadership of a formal terrorist network. Despite this, they attempted to advance plots by conducting training, selecting targets, and procuring weapons.
Overseas Activities Provide Valuable Insight

- Adversaries’ actions overseas foreshadow possible terrorist tactics in the homeland
- Similar overseas experiences and the Internet provide common training opportunities and attack methods
- Intelligence information, web forums, disrupted operations and attacks provide insight into preferred terrorist targets
- Lessons learned from overseas attacks offer security officials in the U.S. insight and perspective for securing similar Homeland facilities
DHS I&A Products

• Roll call releases provide general threat indicators for law enforcement

• Homeland Security Notes provide more specific information based on active threat or activities overseas

• Homeland Security Assessments provide greater analysis of terrorist tactics and targets
Conclusion

- Al-Qa’ida remains the most adaptive and lethal foe but other groups such as AQAP have demonstrated their effectiveness.
  - Targets will be selected for maximum casualties; however, small, easy attacks will increasingly be employed because of the perceived success rate.

- We are concerned that the influence of inspirational figures such as Anwar al-Aulaqi will increasingly motivate homegrown individuals toward violent extremism.
  - Of particular concern are individuals who travel abroad for training and return to attack the Homeland.
  - Individuals motivated by a combination of personal circumstances and external factors, such as grievances over foreign policy, negative ideologues, feelings of alienation, ties to a global pan-Islamic identity, and the availability of extremist propaganda through the Internet and other mass media.

- The Intelligence Community judges that a handful of individuals and small, discrete cells will likely seek to mount attacks each year, with only a small portion of that activity materializing into violence against the Homeland.
Mission

The Philadelphia Police Department’s Homeland Security Unit was established in the spring of 2002 as a proactive response to the elevated threat of terrorism following the attacks of September 11, 2001. Prevent and Respond to potential Terrorism Related and All Hazard incidents.

Although, terrorism prevention was not a new concept for law enforcement, the events of September 11, 2001 emphasized the need for law enforcement to be both first responders & first preventers in the war on terrorism.

Homeland Security Unit
Counter Terrorism Operations
Dignitary Protection/Hostage Negotiations/Investigations
Federal Bureau of Investigation Joint Terrorism Task Force (JTTF)
Homeland Security Unit’s Investigations

- All terrorism related information as well as acts of terrorism or potential terrorism related incidents are fully investigated by experienced Homeland Security Unit investigators.

- These investigators work in unison with the Homeland Security Unit Investigators assigned directly to the Federal Bureau of Investigation Joint Terrorism Task Force (FBI JTTF).

- This collaboration provides both a local and global perspectives on terrorism response and prevention.
Community/Business Support

- Created dedicated Intelligence Center for Counter Terrorism/Crime Prevention and all hazard mitigation supporting the Emergency Operations Center
- Terrorism Prevention Hotline (215) 685-1170
- Website Tip Line www.ppdonline.org
Fusion Partners

A Four State, Twelve County Initiative

- Agriculture
- Banking and Finance
- Chemical Industry
- Community Groups
- Criminal Justice
- Education
- Emergency Services
- Energy
- Government
- Health & Related Services
- Hospitality & Lodging

- Information & Telecommunication
- Military
- Armament Research Development & Engineering Picatinny Arsenal
- Multi Agency Collaborative Environment, Herdon, VA
- Counter Drug Program, Fort Indiantown Gap, US Army Reserve
- Civil Support Team
- Emergency Preparedness Liaison Officers (PPLO) McGuire AFB
- Willow Grove Naval Air Station
- Port Facilities
- Postal & Shipping
- Private Security
- Public Works
- Real Estate
- Retail
- Social Services
- Transportation
Fusion Structure

- NJTTF / HSOC / HNOC / TSOC / RISS
- DIAC
- PaCIC
- NJ ROIC
- MCAC
- USCG FIST
- PHL JTTF FIG
- DVIC
- PORTS / BUSINESS / UTILITIES / HOSPITALS
- LOCAL LE / EM / FIRE
- PUBLIC HEALTH / CAP
- HIDTA / LEJIS / MDA / PARTSWG / LNG / PSN
Homeland Security Unit’s Training

The Homeland Security Unit provides intensive response and prevention training to the Department’s First Responders, who will be the first to arrive on the scene of a major disaster.

To enhance officer safety, training programs include proper Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) techniques, tactics and procedures as well as providing officers with indicators of potential terrorist related activity.

All Homeland Security Unit training programs support the national response strategy and include Incident Command Systems (ICS), and are in compliance with the National Incident Management Systems (NIMS) and the National Response Framework.
Homeland Security Unit’s Major Incident Response Team (MIRT)

- The Major Incident Response Team is the Police Department’s first line of defense in a major disaster or terrorist related event.

- These officers receive specialized training from managing a radiological incident to a natural disaster and are provided with the necessary protective equipment to be effective in major incident management.

- In addition, the Major Incident Response Team meets the department’s short term tactical objectives by providing a specially trained rapid response team, while meeting the department’s long term strategic goals of providing a regional response capability that could be deployed throughout Southeastern Pennsylvania.
Major Incident Response Team

- 500 volunteer officers and supervisors
- Officers receive specialized training in all hazard response, including Weapons of Mass Destruction (WMD)
- Managing Chemical and Biological Incidents
- Decontamination procedures and perimeter security
- Identification of suspects and witnesses
- Primary mission is to secure the warm zone
- Not a special unit (But Special to us)
Philadelphia Police MIRT Equipment-

**Level “C” Protection**

- MSA Millennium APR with NIOSH approved CBRNE Canister and Voice Amplifier
- TYVEK-F Coverall
- Butyl Protective Hood
- Nitrile Gloves and Chemical Resistant Over-Boots
- All Secured with Kappler CHEM-TAPE
- Duty Belt w/sidearm, OC Spray, Handcuffs and Radio
PRIMARY MISSION
Stabilize Conditions

☑ Secure perimeter as needed
☑ Secure the warm zone
☑ Establish order in zone
☑ Identify witnesses and suspects
MIRT PRIMARY MISSION
Stabilize Conditions
ADDITIONAL FUNCTIONS

✓ Assist / contain injured
✓ Identify evidence
✓ Identify secondary devices
✓ Maintain team integrity
✓ Decon prior to leaving warm zone
Homeland Security Unit’s Critical Infrastructure Protection Programs

- The Philadelphia Police Department’s Homeland Security Unit works collaboratively with the U.S. Department of Homeland Security Protective Security Advisors and the Private Sector in developing proactive protective strategies to ensure target hardening of critical infrastructure and critical resources.

- These programs are designed to enhance security while limiting the potential loss of critical services, therefore increasing resiliency.

- Programs include Buffer Zone Protection Plans
- Threat and Risk Assessments
- Site Assessment Visits
Buffer Zone Protection Plans and Vulnerability Assessments

PGW PORT RICHMOND PLANT

Delaware Ave – Facing Southbound from Castor Ave

NO Parking or Stopping in Right Lane adjacent to Plant

Security Recommendation – 1 P/O per tour – Roving Patrol to ensure no vehicles park or stop along or near PGW Plant fence line

PGW Storage Tanks
The Homeland Security unit maintains a compilation of specialized equipment to support the overall mission of terrorism response and prevention, such as a state of the art command and control center.

In addition, the Homeland Security Unit participates in the research and development of merging technologies to be able to provide the best possible tools to our first responders.
Homeland Security Unit’s Community/Business Outreach Programs

It is paramount that the Philadelphia Police Department recognizes the Community/Private Sector as first preventers in the role of crime and terrorism prevention and that both Law Enforcement and the community work in unison to enhance awareness and reduce complacency.

Members of the Homeland Security Unit provide preparedness and prevention training in order to be more efficient and effective in enhancing the safety and security of our communities.

Topics of training include terrorism awareness and indicators, workplace security, bomb threat procedures, suspicious mailings, recognizing explosives and proper procedures for handling packages containing an unknown substance and Active Shooter. All training is tailored to meet specific needs or organizational requirements.
Outreach

Programs:
- Bomb Threat Plans
- Suspicious Mailing Procedures
- Target Hardening

Community Groups:
- Community Awareness Terrorism Training (CAT EYES)
- Terrorism Awareness Training (TAP)
  Designed to create community awareness and report suspicious or unusual behavior
Homeland Security Unit’s Terrorism Leads and Tips Line

- It is critical that the community be provided with a mechanism to report potential terrorism related activity.
- Successful terrorism prevention strategies include disrupting terrorist activity in the planning stages.
- Members of the community are the first to recognize unusual occurrences within their communities that may be indicators of potential terrorist related activity.
- To support the community efforts in reporting suspicious activity, each of the Twenty-Three (23) Patrol Districts throughout the city are staffed with a Terrorism Liaison Officer (TLO).
- In addition, the Homeland Security Unit maintains a Terrorism Leads and Tips line #215-685-1170. As always in an emergency call 911.
Homeland Security Unit’s Agency Coordination

The Philadelphia Police Department’s Homeland Security Unit recognizes the importance of developing true partnerships at the Federal, State and Local levels.

It is critical that emergency responders meet and develop strong relationships prior to meeting the first time at an emergent event.

It is also imperative that these agencies train and exercise joint and individual capabilities utilizing table top exercises, computer simulations as well as full scale training exercises.

To that end the Homeland Security Unit supports all Federal, State and Local initiatives in the development of best practices in the role of terrorism response and prevention.
AGENCY COORDINATION:

US Attorney’s Anti Terror Task Force:
- All Federal, State & local law enforcement agencies represented
- Coordinate the dissemination of information and the development of investigative and prosecutorial strategies throughout the country
- Coordinates training exercises for multi-jurisdictional scenarios
AGENCY COORDINATION:

Southeast Pennsylvania Regional Counter Terrorism Task Force:

- All 5 Counties (Bucks, Chester, Delaware, Montgomery, and Philadelphia) First Responders
- Coordinate the dissemination of Federal Homeland Security Grants and other funding
- Serve as a standing organizational structure for a coordinated response to a terrorist incident in this area.
Intra-Agency Cooperation

City of Philadelphia Working Group: Emergency Management - Police, Fire, and Health Departments
• Recognize the critical value of working with the private sector.

• Center City District - business improvement districts - public / private partnerships - sharing crime data, safety ambassadors standing joint roll calls with PPD, developing unified strategies for enhancing safety.

• RSAN/Alert Philadelphia – emergency text messaging communication system.

• Philadelphia Crime Prevention Council – 270 federal, state & local law enforcement meeting with corporate & private security bi-monthly.

• Building Owner’s & Managers Association’s (BOMA) – Safety & Security Committee – Bill Kelhower is Co-Chairperson.

• ATAC, Joint Terrorism Task Force, Intelligence Centers, Critical Infrastructure.

• Role of private sector in drills, table top exercises, sharing information & tech expertise.
Target Rich Environment

All the things that make Philadelphia a great city, make us a viable target:

- Liberty Bell and Independence Hall - national treasures
Target Rich Environment

Critical Infrastructure

Utilities and Interstate 95
ACTIVE SHOOTER
ASSASSINATIONS
TERRORIST OPERATIONS
MASS KILLINGS
BOMBINGS
ARSON ATTACKS
HIJACKING
STAND-OFF ATTACKS
SUSPICIOUS MAILING (Suspected Explosives)

Protruding Wires
Oily Stains
Lopsided
Strange Odor
No Return Address
Misspelled Words
Excessive Postage
Restrictive Markings
SUSPICIOUS MAILING
(Non Explosive)
ANTHRAX LETTER

4TH GRADE
GREENDALE SCHOOL
FRANKLIN PARK N.J. 08852

SENATOR LEAHY
433 RUSSELL SENATE OFFICE
BUILDING
WASHINGTON D.C. 20510-4502
ROUTES OF EXPOSURES

Inhalation

Ingestion

Absorption

Injection
BIO vs. CHEM TERRORISM

- Not immediately obvious.
- May take days or weeks to notice results.
- Multiple victims with similar symptoms over time
- Eg. Anthrax

- Immediate results
- Multiple victims with similar symptoms almost immediately upon exposure
- Personnel must consider evaluating safety of scene (PPE)
- Eg. Chlorine, Cynide
SHELTER IN PLACE

- Atmosphere outside is more dangerous than inside
- Remain at street level or above (Some agents heavier than air)
- Area should be large enough to support people
- Few doors / windows
- Comfort considerations
- Plastic sheeting & duct tape
- Time?
- HVAC Systems
- Communications – Cell Phones, Radios, Flashlights, Medications, people with special needs, signage.
- Prior Drills and exercises necessary for success.
- Tabletop exercises recommended
Weapons of Mass Destruction Threat Spectrum

- Chemical Weapons
- Radio-Isotopes
- Biological Agents
- Industrial Chemicals
- Explosives

Threat Spectrum:

- LOW
- HIGH
EXPLOSIVES

- 70% of all terrorist incidents involve explosives
- They can be used to disperse chemical, incendiary, or radiological materials
SUI CI DE BOMBERS
Suicide Bomber and Suspicious Device
IMPROVISED DEVICES
SATCHEL DEVICES

CENTENNIAL PARK DEVICE
Exterior view

Letter bombs

Interior view

IED (Improvised Explosive Device) contained black powder with light bulb filament initiator

Once insulation was removed between two contact points – IED functioned.
IED with friction pull initiation system

Once wire/string is pulled – IED functions
Exterior view

Suspect briefcase

Interior view

Cell phone initiated IED
Pipe bombs & bolts utilized as shrapnel
Unabomber Device
Incendiary Devices

Components
- Ignition Source
- Combustible Filler
- Housing or Container

Common Materials Used
- Roadway Flares
- Gasoline/Motor Oil
- Light Bulbs
- Matches/Fireworks
- Electrical Components
- Propane Cylinders
- Bottles, Cans, Plastic Pipes
VEHICLE BOMBS
Together Making The Region Safer!

Thank you.

Captain Walt Smith, Commanding Officer
Homeland Security Unit, Philadelphia Police Department
Police.CO_dom_prep@phila.gov
Phone: (215) 685-1170
L-3 COMMUNICATIONS is a prime contractor in:
• (C³ISR), Command, Control and Communications, Intelligence, Surveillance and Reconnaissance
• Government Services
• Aircraft Modernization and Maintenance (AM&M)
• The broadest base of Electronic Systems in the industry
• L-3 is also a major provider of homeland defense products and services for a variety of emerging markets.