Volume 2, Issue 2
September/October 2010

Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs

DCIP News

DEFENSE CRITICAL INFRASTRUCTURE PROGRAM

THIS ISSUE

The DASD Speaks.....1
Government & Industry in Philadelphia.....3
Vulnerability Assessment Process.....4
HDRAM & The National Guard.....6
Transportation Sector Outreach.....7

NOTES OF INTEREST

- *Next DCIIS: 26-27 January 2011, DLA*
- *DIB CIP: Tentatively Apr/May 2011*
- *Next Newsletter: March 2011*

PCII and You

Got critical infrastructure responsibilities? Need critical infrastructure information for homeland defense responsibilities, but private sector partners hesitate to give you information because they're worried about Freedom of Information Act (FOIA) release to media and competitors? Contact the DoD Protected Critical Infrastructure Information (PCII) Program Office to find out how easy it is to protect lawfully private sector information from public disclosure.

E-mail info-pcii@osd.mil or call 703-699-5710 for information on the DoD PCII Program.

Q. Since assuming your position, what challenges have you found the most difficult to address regarding Mission Assurance?

A. Mission Assurance is the DoD's ability to carry out its mission essential functions in normal conditions, as well as in a stressed or disrupted environment. For me, the biggest challenge is collaboration. If I limit my focus on what DoD owns, and an attack cuts off DoD's power supply at key facilities, how have I helped assure DoD's critical missions? We need to build partnerships, and look for common solutions to help fill these potentially decisive gaps. A large challenge with correcting these gaps is understanding the interdependencies in Critical Infrastructure systems as these interdependencies go far beyond what we in DoD own and control.

Questions & Anwers

Interview Questions with DASD Michael McDaniel, Deputy Assistant Secretary of Defense, Strategy & Force Planning

Q. What are the ASD's CIP priorities? What are your priorities?

A. We have to go beyond just identifying threats and vulnerabilities. We need to address them. The ASD is particularly focused on remediation of Defense Critical Asset (DCA) vulnerabilities, energy grid security, cyber security and information sharing with the DIB, identification of interdependencies with a focus on those in sectors outside of DoD control that affect our ability to perform critical missions (e.g., transportation), and improved interagency coordination/information sharing.

To support the ASD, I want to coordinate various types of assessments to reduce the burden to owners/operators and increase information sharing with DCIP partners. Additionally, we need to increase the following: remediation of known vulnerabilities; system-wide analysis of vulnerability trends, best practices, and dependencies; and system-wide "linkages" such as threats, vulnerabilities and remediation.

(continued on page 2)

Questions & Anwers Continued from page 1.

Q. In your opinion, how does CIP need to evolve at the national level to remain effective in a fiscally constrained environment?

A. At the end of the day, we must understand interdependencies and how we address them as a nation is key. The rewrite of HSPD-7 is a key component of continued CIP evolution. At the national level, we need to address the lack of coverage of cyber issues and have a clear understanding of the term "resilience" and its implications for the execution of essential activities in a degraded environment. In addition, we have to tie the language of critical infrastructure to HSPD-8 to ensure we cover all facets of national preparedness. HSPD-8 establishes mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and it outlines actions to strengthen preparedness capabilities of Federal, State, and local entities.

There are several goals that I have for the revised HSPD-7 that will address this. First, incorporate infrastructure resilience in a well-articulated way that captures the notion of maintaining the ability to execute operations in a degraded environment. Second, clearly identify the distinctive roles of DHS and the various Sector Specific Agencies, maintaining the collaborative nature of the national infrastructure protection enterprise. Third, preserve and strengthen the approaches and mechanisms enabling the public-private partnership. And finally, preserve DoD focus on maintaining internal understanding of infrastructure critical to mission execution.

We also need a clear delineation of roles and responsibilities for the Department of Homeland Security and Sector Specific Agencies. Without it, we could undermine the collaborative nature of the partnership by planting the seeds for inefficiencies and duplication of effort. What we want to avoid is adversely impacting the bottom line of our private sector partners and degrade our carefully established partnership relationship.

Q. With regard to the Defense Industrial Base (DIB), what steps can DoD take to improve its relationship with private industry?

A. A strong relationship with the private sector is in the best interest of our national security. Our ability to respond in a crisis is tied to our reliance on the private sector to use their expertise, flexibility, and technological as new challenges develop. We must maintain the momentum we have built with private sector through our recent DIB CIP Conference and Sector Coordinating Council meetings. The Private Sector is our largest supplier of equipment and parts that support our military mission throughout the globe. It is impossible to separate impacts to private industry from mission accomplishment. One focus area is cyber security. Our ability to function on every level is increasingly linked to cyber security.

For example, the DoD's DIB Cyber Security and Information Assurance Task Force (CS/IA TF) is working in close cooperation with several DIB partners to secure their corporate computer systems and the networks used to store and move unclassified DoD program information. Their work to date has focused on a small number of volunteer companies, but their effort will expand to a much larger group throughout the course of the next fiscal year. It is producing exciting results, providing greater security to DIB information systems, and providing our private sector partners with much needed threat information they can use to counter this persistent threat.

Q. How do you define resiliency and why is it so important to the DoD mission?

A. From our perspective, resiliency is the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions according to the National Infrastructure Protection Plan (NIPP). In layman's terms, it means that we cannot protect everything, so in our preparedness efforts, we have to account for the fact that attacks will happen, mother nature will continue to send major events our way and cyber criminals will act with greater and greater resolve to gain access to our networks and systems. Yet, at the same time, our nation's security depends on the goods and services we and the DIB provide. As a result, we must become a more resilient nation with a resistant infrastructure. We will continue working to that end, but above all, mission assurance activities must contribute to increased resiliency for critical assets and support systems upon which DoD depends.

Q. How can we continue to strengthen the relationship between DoD and DHS with regard to protecting the nation's critical infrastructure?

A. DOD is doing a great deal to support Department of Homeland Security (DHS) in executing their mission and vice versa. I recently had the pleasure of attending the CIKR Asset Protection Technical Assistance Program (CAPTAP) Conference with Assistant Secretary Todd Keil. Mr. Keil reinforced to the State and local attendees the need to grow beyond the beltway and concentrate our focus on the communities and companies that form the foundation of our mission. I wholeheartedly agree with this approach and realize that our relationship with DHS is central in protecting the nation's critical infrastructure. He also emphasized his vision regarding resilience that was in step with my way of thinking. Our work in tandem with public-private partnerships will help facilitate planning, establish effective coordination mechanisms, and build public awareness.

Defense Industrial Base Critical Infrastructure Protection Conference

Joint Effort Results in a Successful Event

"Joint Effort Results In A Successful Event"

Co-hosted by the National Defense Industrial Association (NDIA), Defense Contract Management Agency (DCMA), and the Office of the Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs (OASD(HD&ASA)), the fourth annual Defense Industrial Base (DIB) Critical Infrastructure Protection (CIP) Conference was held April 26-28, 2010 in Philadelphia, PA. The DIB Sector conducted related activities during the event, including holding meetings of the Sector Coordinating Council and Defense Security Information Exchange, and convening the Critical Infrastructure Partnership Advisory Council (CIPAC). These proceedings are part of a multi-faceted outreach strategy through which DoD, as the DIB Sector-Specific Agency (SSA), reaches out to sector partners and other CIP stakeholders to promote the health and well being of the sector. The conference was opened by Dr. Paul Stockton of DoD and Todd Keil, Assistant Secretary for Infrastructure Protection, Department of Homeland Security. They both expressed the importance of improving relationships with private industry. Reinforcing the conference theme of "Risk Reduction & Mitigation in the Defense Industrial Base," these two speakers discussed their respective responsibilities in CIP and how they envision the way ahead for mutual support and cooperation across all sectors. They addressed an audience including representatives from the White House, Department of Homeland Security (DHS), the Los Angeles Joint Regional Intelligence Center, and several other organizations representing Federal and State governments.

Various panels and guest speakers, representing a myriad of organizations, responded to statements and questions from their moderators and the audience on topics ranging from resilience to exercises. This format inspired a roundtable of different perspectives generating a high level of interaction. Individual speakers highlighted potential economic impacts and threats to the DIB. These briefs provided insight on the unique nature of outside influences across the industrial base. Mr. Ed Halibozek, Vice President of Security, Flight Operations and Administration for Northrop Grumman, addressed the importance of corporate contingency planning in his industry keynote address. He reminded the audience that advance planning and applying a flexible focus in times of crisis lead to business resiliency. He cited the Northrop Grumman cybersecurity operations center as an example of those concepts in practice. The participation of local entities (e.g., emergency management, law enforcement) and regional private sector partners enhanced the level of discussion during the conference, linking wider issues to real-world situations and available tools and resources. The conference included perspectives from within the sector but also emphasized the importance of understanding interdependencies with other sectors.

The conference offered numerous opportunities to share ideas, network, and discuss how the collective engagement of DIB stakeholders is essential to the long-term investment in the resilience of our Nation. With the help of DHS and other partners, these events will continue to provide an effective venue to present and discuss concrete ideas for improving CIP to enhance the DIB's ability to maximize sector resilience.

The conference proceedings are available online: http://www.dtic.mil/ndia/2010DIBCIP/2010DIBCIP.html.

USSTRATCOM and Space Sector Vulnerability Assessment Support

By Mr. Martin Bixby and Mr. Gil Dysico

The identification of Task Critical Assets (TCAs) is only one step in the Defense Critical Infrastructure Program (DCIP) risk assessment process. Another key component is the vulnerability assessment.

DoDD 3020.40 defines vulnerability as a weakness or susceptibility of an installation, system, asset, application, or its dependencies that 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.

To facilitate this process, US Strategic Command and the DCIP Space Sector are working closely with the Defense Threat Reduction Agency (DTRA) Balanced Survivability Assessment (BSA) and Joint Staff Integrated Vulnerability Assessment (JSIVA) teams, Geographic Combatant Commanders, Installation Commanders, and Services to: nominate installations, develop assessment focus statements (AFS), coordinate assessment notification with installation leadership and personnel, augment vulnerability assessment teams, and track/influence remediation efforts.

USSTRATCOM and the Space Sector have found the following best practices for facilitating the planning and execution of the assessment:

Assessment nomination process

- *Conduct an annual review of installations with TCAs that have not been assessed by a Service or DTRA assessment team in the past three years.*
- *Collaborate with the Geographic Combatant Commands (COCOMs); Agencies, other Sectors and Services to gain broad support for nominations and ensure limited assessment resources are optimally used.*

Participation in pre-assessment visits/notification

- *Conduct site surveys with the Geographic COCOMs and assessment teams to validate assets and identify inter-dependencies prior to the formal assessment. This "pre-visit" fosters relationships and dialogue with on-site personnel and command staff.*
- *Provide the installation leadership a DCIP overview to explain the importance of TCAs on the installation along with the goals, processes, and benefits of the assessment. Installation leadership is often not aware of how important some assets are to DoD.*

Assessment Focus Statements (AFS) development

- *Work closely with the Geographic COCOMs to ensure that both regional responsibilities and UCP missions are considered in the input.*
- *Ensure Command/Sector equities are thoroughly addressed, and all applicable Joint Mission Essential Tasks are included to provide mission threads to missions and functions.*
- *Recently we've had great success by providing the Geographic COCOMs an AFS that has been signed by USSTRATCOM senior leadership. This serves to reinforce the assessment's importance.*

Augment DTRA assessment teams

- *Provide on-site assistance to the assessment teams and ensure AFS objectives are accomplished.*
- *In coordination with the assessment team, examine and document findings in accordance with the assessment benchmark standards or industry best practices.*
- *Examine AT/FP, networks, cyber considerations as described in the AFS, with particular attention to the inter-dependencies.*

Incorporate findings and recommendations presented to installation leadership in risk determination

- *Assist the assessor in interpreting the findings and specifying the reference standard which the deviation or vulnerability is measured against.*
- *Ensure that the organization responsible for remediation is identified and included in the final report. Without this, remediation often does not occur.*
- *Track the final report (should be issued within 60 days).*
- *Track/influence implementation of report recommendations and provide leadership a summary of findings documented during the assessment.*

Continued from page 4.

USSTRATCOM and Space Sector Vulnerability Assessment Support

By Mr. Martin Bixby and Mr. Gil Dysico

The assessment final report defines vulnerabilities indentified as follows:

- **High:** Indicates that exploitation of the asset's vulnerability would have ***grave consequences*** resulting in mission failure.
- **Medium:** exploitation of the asset's vulnerability would have ***serious*** consequences resulting in loss of classified or highly sensitive data or equipment/facilities that would impair operations for an indefinite amount of time.
- **Low:** exploitation of the asset's vulnerability would have ***moderate consequences*** resulting in loss of confidential and/or sensitive data or costly equipment/facilities that would impair operations for a limited period of time.
- **Marginal:** exploitation of the asset's vulnerability would have ***little or no impact*** to continuation of operations.

This year USSTRATCOM and the Space Sector are participating in vulnerability assessments at U.S.-based and foreign-based DoD installations and will use assessment results as a key component in the risk management decision packages that will be presented to Command leadership.

Additionally, USSTRATCOM and Space Sector personnel attend JSIVA Mobile Training Team (MTT) assessment courses to expand their knowledge of the DTRA assessment process and standards. USSTRATCOM and Space Sector personnel have also been asked by the Joint Staff and DTRA to augment the training teams by providing Strategic Mission Assurance Data System (SMADS) training to installation Anti-Terrorism Officers (ATOs) during selected MTTs. This will make ATOs more familiar with SMADS and facilitate TCA incorporation into mission essential vulnerable areas (MEVAs) and associated installation defense plans.

Finally, USSTRATCOM and the Space Sector stand ready to work with others in the DCIP community who wish to become involved in the vulnerability assessment process.

Homeland Defense Risk Analysis Model: An 'All-Hazard' DCIP Tool for the National Guard

By: Mr. John Gassler, NGB/J-34 CIP Branch

In December of 2003, Homeland Security Presidential Directive 7 (HSPD 7) established U.S. policy for enhancing protection of the Nation's vast network of Critical Infrastructure and Key Resources (CI/KR). Consequently, HSPD 7 directed Federal departments and agencies to identify, prioritize and coordinate the protection of CI/KR to prevent, deter and mitigate efforts to destroy, incapacitate or exploit everything from bridges and dams to manufacturing and chemical plants.

Needing an umbrella plan or national strategy that spoke directly to Defense Critical Infrastructure (DCI) protection, the National Infrastructure Protection Plan (NIPP) was put into place as the driving force or mandate for HSPD 7 policy implementation. Subsequently, Department of Defense Directive (DoDD) 3020.40, "Policy and Responsibilities for Critical Infrastructure," hammered out operating procedures and key tasks for successful execution of Defense Critical Infrastructure Program (DCIP) roles assigned to agencies like the National Guard Bureau (NGB).

Successfully piecing together the entire DCIP mosaic is complex and challenging. Policy development, management and critical asset identification are just parts of the overall DCIP process. Recognizing that a vital need exists to systematically identify infrastructure-based vulnerabilities and then mitigating defined risks, the NGB is moving forward with development of an "all-hazard" risk assessment tool called the Homeland Defense Risk Analysis Model (HDRAM).

"The vision, necessity and driving force behind the application and development of HDRAM is the ability to compare like and dissimilar critical infrastructure in a variety of NIPP sectors, a variety of threats and hazards (natural and man-made) with a sophisticated tool that is scientific, objective, quantifiable, fast, repeatable and defendable," said Colonel Thomas McGinley, Provost Marshal for the NGB Joint Staff.

HDRAM's genesis began with the U.S. Coast Guard, a process and a refined, seventh generation tool they use for port/maritime critical infrastructure risk assessment called the Maritime Security Risk Analysis Model (MSRAM). MSRAM, a terrorism-based risk analysis tool used by every Coast Guard Captain of the Port (COTP), enables federal maritime security coordinators and Area Maritime Security Committees to perform detailed scenario risk assessments on all of their maritime CI/KR. MSRAM assesses risk based on scenarios --- a combination of target and attack mode --- in terms of threat, vulnerability and consequence.

The MSRAM tool has been met with stellar success, and through a newly signed Memorandum of Understanding (MOU), the U.S. Coast Guard has offered to share their tool with the NGB and assist with the migration and adaptation of the MSRAM methodology for its shoreside, all hazards critical infrastructure protection needs.

"Sharing and converting MSRAM into HDRAM is important for many reasons; one of them is capitalizing on technologies and processes that already exist and have already been tested and successful used in the field. Additionally, we're growing operational synergies between the U.S. Coast Guard and the National Guard Bureau," stated Commander John Hooper, U.S. Coast Guard liaison to the NGB/J-34 CIP Branch.

The concept behind HDRAM is simple: provide a tool for the Several States that is all-hazard centric. Slated to be spearheaded from each State's Joint Force Headquarters (JFHQ), the HDRAM tool will allow for cross-sector comparative analysis of CI/KR. "The 'payback' for the U.S. Coast Guard in this joint endeavor is that it will be able to capitalize on any lessons learned, best practices, and software development as the National Guard transforms this tool to meet its needs. Undoubtedly, there will be new processes and procedures that, once integrated, will enhance subsequent MSRAM iterations and could indeed find applicability in other U.S. Coast Guard mission sets," added Commander Hooper.

Still a fairly young government initiative, the DCIP is a recognized and highly visible program of record with an extremely vibrant future. HDRAM, in turn, seeks to provide the software tool both the Army Guard and Air National Guard can use to prioritize and assess critical infrastructure. From hurricanes and floods to tornadoes and terrorist attacks, HDRAM is the NGB's DCIP vision for the future.

Transportation Sector Strengthens Partnership with Federal Government and Private Industry through Outreach

When a catastrophic 7.0 earthquake hit Haiti on January 12, 2010, United States Transportation Command knew they would be heavily engaged in providing relief to the Country of Haiti. Once President Obama gave the order for DoD to provide assistance, the Haiti crisis quickly became Operation Unified Response. Key to the success of Unified Response was going to be transportation infrastructure in the southeastern United States and in particular, the port of Jacksonville Florida. Jacksonville's location is at the crossroads of three major railroads (CSX, Norfolk Southern and Florida East Coast Railway) and three interstate highways (I-95, I-10 and 1-75) and the Port of Jacksonville's Blount Island and Talleyrand Marine Terminal.

For Operation Unified Response, the Talleyrand Marine Terminal was prepared to handle 270 cargo loads of humanitarian assistance material per day but was told the total required would be closer to 800 loads. Hence, in order to handle the surge, they would also have to use Blount Island, which is about 10 miles from Talleyrand. After all was said and done, USTRANSCOM coordinated, on average, the movement of more than a million pounds of relief supplies, food and water into Haiti every single day from January 16th until March 3rd, 2010. Behind the scenes of this massive logistical achievement were professional relationships between federal, state and local partners in the transportation sector.

Maintaining and developing those relationships is why the Office of the Assistant Secretary of Defense (OASD) for Homeland Defense and Americas Security Affairs (HD&SA) is focused on their Sector Leads going out into their respective sectors and promoting awareness of the roles and importance of Defense Critical Infrastructure and fostering relationships among the DoD, Interagency counterparts and private sector partners.

USTRANSCOM is the Transportation Defense Infrastructure Sector Lead Agent and one of the responsibilities is to assure the availability of military and commercial infrastructure critical to the Joint Deployment Distribution Enterprise (JDDE) in an all-threat and all-hazards environment. The JDDE is largely comprised of commercial and federal partners. The USTRANSCOM Critical Infrastructure Program (CIP) Program Manager, Mr. Wayne "Jake" Carson is focused on his team reducing or mitigating unacceptable risk to transportation infrastructure. The CIP outreach program specifically focuses on JDDE partners responsible for transportation infrastructure on a global scale. This past September, Mr. Carson and two of his Risk Analysts; Mr. Bob Ross and Mr. Cipriano Pineda, took a trip to the Ports of Jacksonville, Florida and Savannah, Georgia to conduct CIP outreach and promote the Transportation Sector CIP within the Southeastern region. This trip in particular offered a great opportunity to build on existing relationships with commercial rail and maritime infrastructure asset owners in the Southeastern region of the United States and learn about planned infrastructure improvements at those respective sites. The outreach team met with the officials of the Jacksonville Port Authority, the U.S. Marine detachment at Blount Island Terminal, CSX (Railroad) headquarters and met with representatives of the Jacksonville Chamber of Commerce. At every meeting, the role of USTRANSCOM as the DoD Transportation Sector Lead was explained and there was a healthy exchange of information that was mutually beneficial to all parties. The team then travelled north to the Savannah, Georgia region meeting with the Port of Savannah and Fort Stewart, Georgia officials to discuss deployment and redeployment operations. Outreach with the installation transportation officials at Fort Stewart included increased awareness about transportation infrastructure on and off the installation. Once again, important information was exchanged and all organizations benefitted from the meetings.

This trip provided an excellent opportunity for the USTRANSCOM CIP team to gain additional knowledge on transportation infrastructure within this region of the U.S. Mr. Carson is confident the USTRANSCOM CIP outreach program will pay dividends during routine operations and also during any unforeseen crisis when DoD is quickly called for help in a time of need, such as Operation Unified Response. Most importantly, the USTRANSCOM CIP team continues to strengthen existing partnerships with our private industry and transportation partners at locations that play a significant role in the Joint Distribution Deployment Enterprise.

Port of Jacksonville

CIP Related Conference Schedule

-

National Symposium
26 - 29 October,
Colorado Springs, CO

-

Optimizing Investments in CIP Conference
15 - 18 November,
Arlington, VA

-

CIP Congress
30 Nov - 2 Dec
National Harbor, MD

>Need Access to the DCIP Web Portal?

Just send an email to george.davidson.ctr@osd.mil with your organization and ten digit EDIPI CAC number, which is the number you see on your computer screen when you withdraw your CAC (For Example: 2347659871@mil). Once the information is received, it will take 48-72 hours to process. There is no longer a username/passsword for the DCIP web portal.

>DCIP Education, Training and Outreach (ETO) Website

The DCIP Education, Training and Outreach (ETO) Website is currently under development. This website will be hosted by the Deffense Technical Information Center and will not require a Common Access Card.

DCIP GOALS

- Provide DCIP Policy and Program Guidance
- Foster DCIP Strategic Partnerships and Enabling Technologies
- Integrate & Implement DCIP Plans, Programs and Capabilities
- Facilitate DCIP Resourcing
- Promote DCIP Education & Outreach

DCIP OFFICE
Phone: 703 602-5730
Email: RSS.DCIPOffice@osd.mil

Articles that appear in this newsletter do not necessarily represent the views of or are endorsed by HD&ASA.