Volume 1, Issue 2
November 2009

THIS ISSUE

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

DCIP News

DEFENSE CRITICAL INFRASTRUCTURE PROGRAM

POINTS OF INTEREST

- *DIB CIP tentatively planned for April 2010 in Philadelphia, PA*
- *Next DCIIS will be held May 2010 - Location TBD*
- *Next Newsletter: March 2010*

FROM THE DIRECTOR

I am pleased to announce my official acceptance of the position of Director, Defense Critical Infrastructure Office for Homeland Defense. I appreciate the kind words and congratulations I have received thus far and look forward to working with everyone in the future as we continue to develop this program.

In early September, we completed our annual Program Reviews. The participation of your staffs along with your excellent presentations have provided me the necessary insight to help shape my decisions for the upcoming year. It was particularly informative to learn of the priorities and challenges facing the community as a whole. To resolve these matters, I request your continued assistance in maintaining our two-way, open communication to cultivate thoughts and ideas for more efficient execution of our mission. With that in mind, the ASD has made it clear that the DCIP is a top priority. Furthermore, under the direction of our new DASD for Strategy & Force Planning, Mike McDaniel, we can expect a high level of interest in how we are striving to meet DCIP goals and objectives.

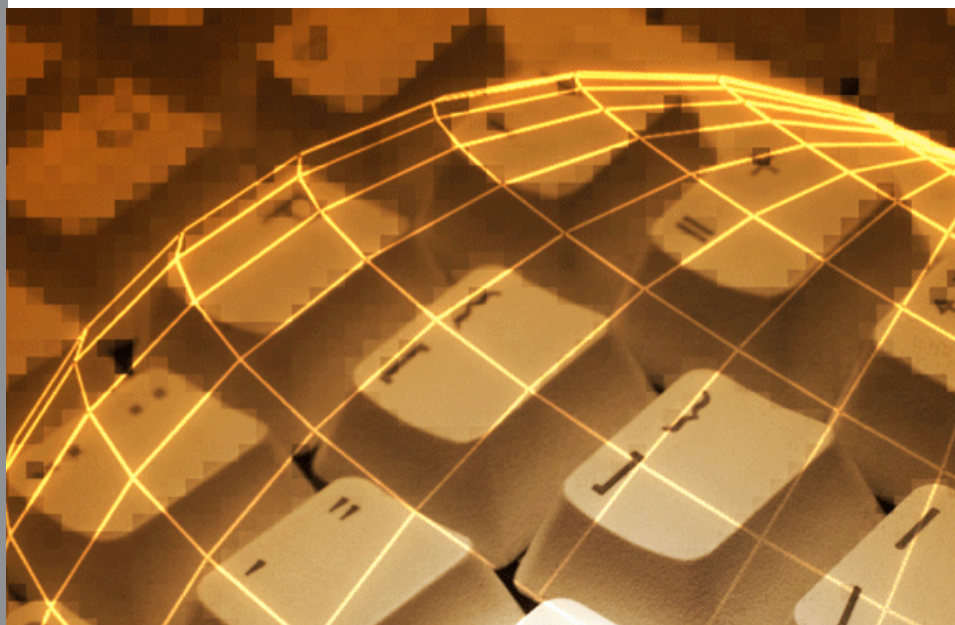
From Program Reviews to funding requests, October marked the transition of a new fiscal year. I appreciate the time and effort taken to submit prioritized and important resource requirements in a timely fashion. Your patience and cooperation is appreciated as allocating limited resources to the utmost benefit of the program is always a challenge.

By the time this newsletter is published, we will have completed the final DISC and DCIIS of 2009. As one of the initiatives for 2010, we will hold these events semi-annually vice quarterly. This decision was based on feedback from the community to help alleviate travel demands in our fiscally restrained environment. The DCIP community has made tremendous strides over the past year. With improved guidance, increased awareness, and dedicated support, we will continue to enhance the safety of our nation well into the future. As always, thank you again for your valued inputs and hard work.

Jamie Clark
Director
Defense Critical Infrastructure

Mission Assurance: Looking Forward

The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs has directed the development of an overarching Mission Assurance (MA) strategy to strengthen DoD's ability to execute its essential functions in the face of natural catastrophes or attacks, including strikes against defense critical infrastructure. MA links numerous diverse risk management programs, activities, and security related functions to ensure accomplishment of the Mission Essential Functions (MEFs) of the Department. The desire is to provide an integrating framework for complementary programs, functions, and activities. With MA being implemented at various levels throughout the DoD, it is important to evaluate what strategic direction is necessary to ensure continuity of purpose for this initiative.



PCII and You

by Anne La Lena OASD (HD & ASA)

SABER ES PODER Knowledge is power – and information is the core of knowledge. Regardless of your job, you need information to do it. If your job involves homeland defense and critical infrastructure, you not only need information, you may need a particular type of information – Protected Critical Infrastructure Information (PCII) – and PCII and the DoD PCII Program may help you do your job even better.

PCII refers to a type of critical infrastructure information (CII) voluntarily given by the private sector to the Federal Government for homeland security/homeland defense use which qualifies for protection from public release and safeguarding to ensure appropriate use. The private sector owns the preponderance of the Nation's critical infrastructure -- estimates range from 85 percent to 95 percent – and its business sensitive CII may be needed for vulnerability assessments, risk mitigation, dependency analyses, or other homeland defense responsibilities, yet may not be readily available because of concerns of competitor access or general public release. PCII is proprietary, business sensitive, and confidential private sector information that is not customarily found in the public domain – and which is statutorily protected from release to the public domain per requests under the Freedom of Information Act, and similar State and local government disclosure laws. PCII is also protected from use in civil litigation or as a basis for regulatory action, per the Critical Infrastructure Information Act of 2002 (CII Act).

The DoD PCII Program, based in the Defense Critical Infrastructure Office, facilitates access to and is the lead office for PCII for the Department, and is an accredited partner with the Department of Homeland Security (DHS) in the PCII Program, where proprietary, business-sensitive, and confidential CII is validated and marked as PCII. To gain the protection of the CII Act, private sector information must meet a few simple requirements.

The DoD PCII Program facilitates access to PCII in several ways, notably:

- ***Working with your office to implement the required safeguarding and use procedures after training, and***
- ***Developing a special arrangement whereby the private sector will provide its CII directly to your office for immediate access and use, and it is validated as PCII upon receipt. This arrangement is known as a Categorical Inclusion arrangement and must be negotiated with DHS prior to CII being provided to a DoD Component for protection under the CII Act.***

As participation by the private sector is voluntary, the specific information needed by your office may not be available. The Categorical Inclusion arrangement is an avenue that can be used to develop an information sharing partnership with the private sector to gain that information. Before gaining access to PCII, DoD personnel are thoroughly trained in the proper use and handling requirements for PCII.

US Strategic Command and the Defense Contract Management Agency are active in the DoD PCII Program. For more information, contact us at: 703-602-5730 ext. 147; or e-mail: info-pcii@osd.mil or Anne.LaLena.ctr@osd.mil.

"The private sector owns the preponderance of the Nation's critical infrastructure -- estimates range from 85 percent to 95 percent"

Strength Through Resilience

"The DSAT is an interactive SIPRNET-based tool, developed to provide Installation Commanders and asset owners with the ability to perform their own DCIP self-assessment."

DCIP Self-Assessment Tool (DSAT)

by Raymond Moon, DON CIAO

AS OTHERS IN THE DOD, the Department of Navy (DON) relies on a network of physical and cyber infrastructure so critical that its degradation, exploitation, or destruction could have a debilitating effect on the DON's ability to project, support, and sustain its forces and operations worldwide. This critical infrastructure includes DON and non-DON domestic and foreign infrastructures essential to planning, mobilizing, deploying, executing, and sustaining U.S. military operations on a global basis. DON critical infrastructures, physical or cyber, must be available when required.

Historically, the approach to critical infrastructure protection (CIP) within the DON has focused on physical infrastructure, and largely aligned with antiterrorism efforts utilizing boots on the ground assessments. However, recognizing the fact that there was not adequate vulnerability assessment coverage, the DON embarked on the development of a CIP Self-Assessment Tool (CIP SAT). CIP SAT allows the assessment of those critical assets identified through the Critical Asset Identification Process (CAIP) to determine potential vulnerabilities. At the request of the ASD(HD&ASA), the DON is enhancing CIP SAT to produce a Defense Critical Infrastructure Program (DCIP) Self-Assessment Tool (DSAT) that OSD will make available to all DoD.

The DSAT is an interactive SIPRNET-based tool, developed to provide Installation Commanders and asset owners with the ability to perform their own DCIP self-assessment. The DSAT enables a thorough reporting of an installation's or critical asset's CIP posture, including identifying vulnerabilities that could jeopardize the execution of Mission Essential Tasks (METs).

After identifying installation METs and associated Critical Assets, DSAT presents a series of questions based upon DoD approved benchmarks and standards. DSAT groups and presents the questions in the following five modules:

1. Antiterrorism/Force Protection (AT/FP)

2. Commercial Dependency (CD)

3. Computer Network Defense (CND)

4. Continuity of Operations/Emergency Management Planning (COOP/EM)

5. Chemical, Biological, Radiological, Nuclear, and High Yield Explosive (CBRNE)

DSAT supports four different *levels* of users:

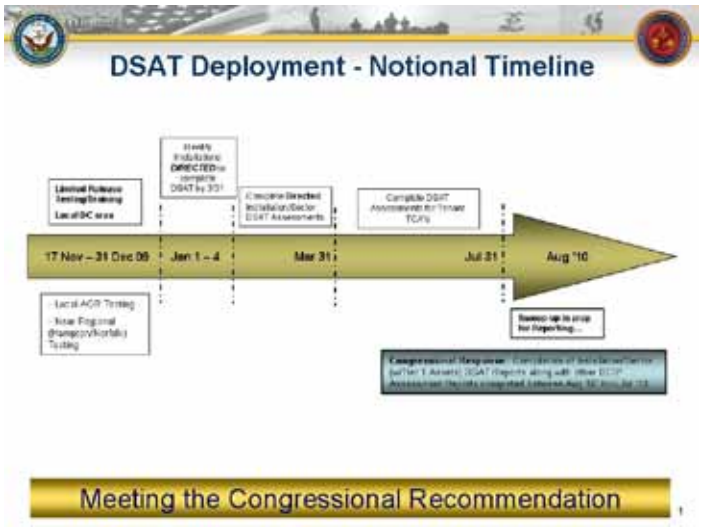
1. Installation Commanders. Installation Commanders are responsible for setting up the self-assessment with situational data and assigning assessors to answer questions (e.g., AT/FP Officer assigned the AT/FP module), monitors in-progress status, and finalizes the assessment by accepting survey answers.

2. Asset Owners/Tenant Commands. Asset owners are responsible for completing a focused assessment of individual critical assets after reviewing the completed DSAT report from their host installation for applicable vulnerability data.

3. Assessors. Assessors are individuals assigned by the Commander to answer DSAT questions. This level also includes those assigned as a Data Entry person.

4. Senior Staff. Senior staff are those in positions above the Installation Commander level, wanting to review recent and archived DSAT reports.

Following certification and accreditation, and initial testing, ASD (HD&ASA) will make DSAT available in the summer of 2010 time-frame to installation commanders and asset owners throughout DoD. ASD (HD&ASA) is developing an implementation plan that will provide more detail of the entire project.



USNORTHCOM Critical Infrastructure Protection Course

by MAJ Eric Choy and Clifford Mullen, Force Protection/Mission Assurance Division

IN EARLY SEPTEMBER 2009, USNORTHCOM J34 Force Protection/Mission Assurance Division hosted the second iteration of US Northern Command's (USNORTHCOM) Critical Infrastructure Protection (CIP) Orientation course. The successful first iteration of this course took place in August 2008 and began as an outreach initiative to components, partner agencies, and North American Aerospace Defense Command (NORAD) & USNORTHCOM (N-NC) directorates to provide training on CIP and the tools to uniformly apply Defense Critical Infrastructure Program (DCIP) policy across the USNORTHCOM Area of Responsibility (AOR).

Twenty-eight CIP Action Officers representing eighteen separate component, interagency, and NNC staff directorates attended the course held at Peterson Air Force Base, Colorado Springs, Colorado. The course objectives were to provide a forum for joint and interagency participation to promote DCIP unity of effort between component and interagency partners; build partnerships that create a mutually supportive and collaborative environment; and strengthen core CIP analytical competencies. These core analytical competencies included CIP event and impact reporting, CIP area characterizations, daily CIP situational awareness, and identification of and risk assessment support for task-critical assets (TCA).

The course is structured upon the building blocks of policy and regulation, CIP tools, and CIP products. These building blocks provide the foundation for the uniform application of DCIP policy and standards; promote DCIP/CIP education and awareness; and open dialogue among DCIP community members across the USNORTHCOM AOR.

This year's course topics were:

- ***DoD DCIP Policy and USNORTHCOM DCIP Guidance Review***
- ***USNORTHCOM Homeland Defense (HD) and Defense Support of Civil Authority (DSCA) and CIP Event Reporting for Critical Infrastructure***
- ***Homeland Security Information Network (HSIN) Review and Training***
- ***Open Source Information (OSINF) Training and Application for Infrastructure Analysis***
- ***DODM 3020.45 V1 - Critical Asset Identification Process (CAIP)***
- ***USNORTHCOM CIP Characterization Analysis Production***
- ***Strategic Mission Assurance Data System (SMADS) Review and Training***

Successful execution of the CIP Orientation Course has furthered USNORTHCOM's efforts to develop partnerships which result in improved information sharing and visibility of Defense Critical Infrastructure. These partnerships have grown beyond USNORTHCOM Components to include the National Guard Bureau; Defense Agencies and Field Activities; Department of Homeland Security Office of Infrastructure Protection; and the National Infrastructure Coordinating Center. Information sharing with key DCIP partners supports the accomplishment of our critical infrastructure protection mission, improves the quality and accessibility of DCIP and critical infrastructure information, and supports the Commander, USNORTHCOM, and the Department of Defense at all levels. Although the format for future iterations of the USNORTHCOM CIP Orientation may change to address current DCIP issues, the focus will always remain on fostering a mutual understanding of the participants' organizational DCIP roles and the collaborative necessity of the DCIP program.

For additional information on the USNORTHCOM Defense Critical Infrastructure Program or the CIP Orientation course contact:
Mr. John Schauffert, Chief, NC/J34 Assessment/CIP Branch at 719-554-7126 , or
MAJ Eric Choy, Deputy, NC/J34 Assessment/CIP Branch at 719-554-7127.

Energy Security Using Strategic Islands

by Dan Mathis, NSWCDD

The electric power grid was designed and constructed to satisfy a different business model and consumer than what is demanded by today's digital customer and profit driven utilities. The bulk power market of today is open and competitive, uses aged transmission lines that need upgrading, and relies on substations that have surprisingly few reserves of long lead time equipment. The grid is maintained to survive operational and not catastrophic events. There is an increased risk of lengthy commercial power outages that will include DoD installations and supporting facilities. With heavy reliance on diesel for back-up generation, availability and longevity of electric power to support continuity of operations becomes an area of increasing concern.

Strategic electric islands can provide electric power energy security for DoD installations and supporting facilities. The island footprint should include the area around the DoD installation, because supporting infrastructures and personnel transcend the installation's fence line. A generation installed on DoD land can be more readily secured from both physical and cyber attacks. Many DoD installations are located in areas that are served by congested transmission lines, which create financial incentives to sell excess DoD-generated power to the grid. Renewable technologies used to power DoD-owned generation will help reach environmental goals and provide energy security.

Depending on the extent of the island footprint and the anticipated installation of new generation and network configuration, partnerships with utilities, generation developers, and the DoD may be required. Developing partnerships will limit investment risk and may prove more financially attractive for the DoD.

A utility may have local generation in the area already, which can be used to power the footprint. For example, in the Norfolk area, the local utility, Chesapeake Energy Center, located approximately 18 miles from the Naval Base Norfolk, produces 760 MW of electric energy. The Chesapeake Energy Center consists of four coal-fired units and eight gas turbines. This base load, augmented by renewable energy technologies (e.g., municipal waste), will provide energy security for the Hampton Roads Peninsula if developed into an electric island.

In areas where there is transmission congestion and no local generation, most utilities welcome a generation source that will avoid the construction of a new transmission line and provide voltage stability for the area. A cooperative effort to install new generation on DoD land will accelerate the permitting process, especially using alternative energy technologies. One option might consist of installing a gas turbine, where waste gas displaces natural gas in stages, as these renewable resources become available. For example, a 130 megawatt gas turbine has a $162 million price of entry, with 4.3 cents per kilowatt-hour associated costs. If the local electricity cost is 11 cents per kilowatt-hour, the return on investment is 48 months.

Numerous islanding implementation options are available, and must be evaluated individually based on a site-specific business case and return on investment analysis. Available data set layers such as renewable resource locations, transmission lines, substations, generation facilities, state renewable tax incentives, transmission congestion corridors, and military installations will identify potential DoD installations that can become part of a strategic electric island.

Strategic Islanding Concept

- Islanding footprint includes military installation(s) and surrounding area.

- "Strategic Islanding" powered by conventional and renewable fuels increases energy security through diversity

- DoD electric power energy security through military and commercial electric utility partnerships.

- Secured DoD generation, powers "the Island" during blackouts and sells power grid during normal conditions.

- Maximized return on investment when DoD owned generation relieves transmission congestion.

CIP Related Conference Schedule

-

TISP Conference
9-10 Dec., Grapevine, TX

-

TCIP Conference
2-4 Feb., Philadelphia, PA

H1N1 Pandemic Table Top Exercise

by LCDR Van Morfit, OASD(HA)/TMA

THE H1N1 PANDEMIC has been the focus of a large number of Table Top Exercises (TTXs) this year. On October 13th and 14th the Health and Personnel Sectors of the Defense Critical Infrastructure Program (DCIP) jointly sponsored an H1N1 TTX in order to examine the connections between the two sectors to see how they will work together and what they can do to improve their responsiveness in response to an anticipated incremental personnel loss up to 40% due to an infectious disease.

Ms. Sally DeSanto and LCDR Van Morfit cohosted the event at the LMI headquarters in Virginia. The 60 plus participants included representatives from both Sectors, the military Services, COCOMs, DHHS, DHS, and SMEs supporting the Health and Personnel Sectors.

This was the first of two planned TTXs with the second planned to occur in early 2010. It will be a larger scale exercise to actively include all members of the DOD DCIP partners as well as DHHS, DHS, VA, and the White House.

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 ext 167
Fax: 703 602-5725

ANNOUNCEMENT
DCIP Video to be released next month!