Volume 2, Issue 1
March/April 2010

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

DCIP News

DEFENSE CRITICAL INFRASTRUCTURE PROGRAM

THIS ISSUE

POINTS OF INTEREST

- *DIB CIP: April 26-28, 2010, Philadelphia, PA*
- *Next DCIIS: June 21-25, 2010, USTRANSCOM*
- *Next Newsletter: June 2010*

WELCOME

New Mission Assurance Director

Beth Cordray
Director, Mission Assurance
(DASD, Homeland Defense
Strategy and Force Planning)
Director Executive Secretariat

CURRENT ASSIGNMENT: Elisabeth Cordray presently serves as the Director for Mission Assurance, where she is responsible for developing strategies, policies, and programs to ensuring the DoD is able to perform its critical missions. Beth is responsible for providing policy advice and leading DoD efforts on mission assurance, anti-terrorism, force protection and critical infrastructure protection issues.

PAST EXPERIENCE: From October 2008 – December 2009 Beth served as special assistant to the Deputy Under Secretary of Defense for Policy Integration and Chief of Staff. As special assistant, she led Policy support for the transition of Administrations, assisted the incoming political leadership establish their strategic priorities and goals, facilitated the realignment of the Policy organization to align to those goals, and led efforts to address key management and support issues on behalf of Policy's leadership.

From Oct 2007- Oct 2008, Beth served as Director, Defense Transformation, Force Planning, and Requirements on the National Security Council staff. In this capacity, Beth advised the Assistant to the President for National Security Affairs on a wide range of defense issues including defense strategic planning, interagency planning, force planning, contingency planning, national security professional development, global defense posture, defense budget, and security cooperation.

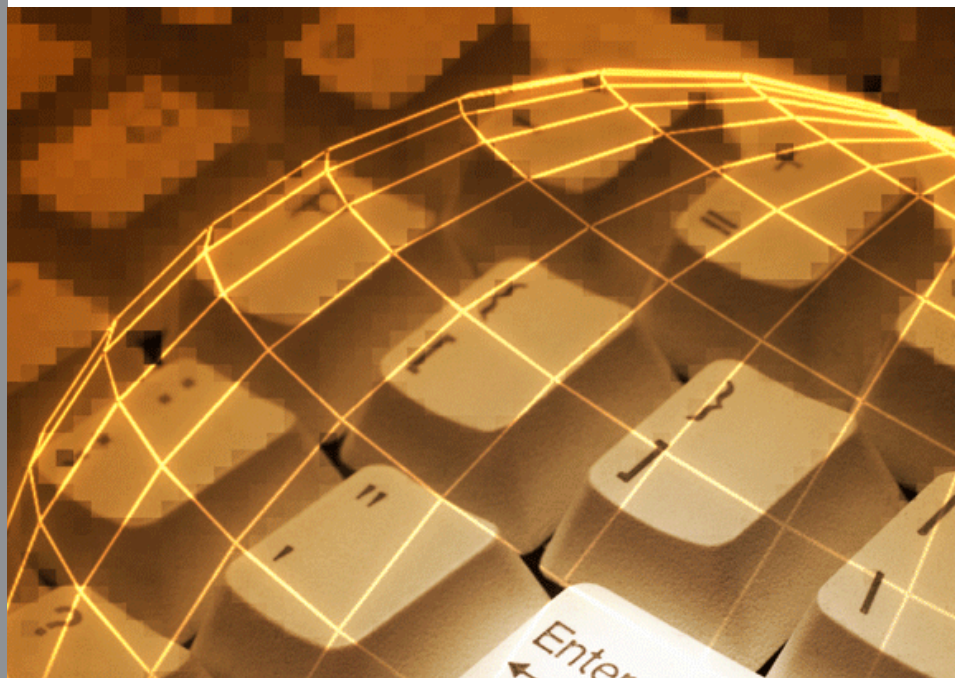
From Jan-Oct 2007, Beth worked for the Deputy Assistant Secretary Defense (DASD) for Partnership Strategy on security cooperation. She lead the development of the 2008 Guidance for Employment of the Force by building a team across Policy, Joint Staff, Services, Combatant Commands, State Department, and USAID. She also initiated several security cooperation reform initiatives.

Throughout the 2006 Quadrennial Defense Review (QDR), Beth was a lead action officer on the QDR Integration Team. Beth assisted defense leaders in examining the range of issues and determining the focus areas, which often required extensive negotiation with key QDR participants across the Department of Defense and from the Interagency. She authored portions of the QDR Terms of Reference, developed the conceptual outline for revising the force planning construct and contributed to the final QDR Report, as well as the Strategic Planning Guidance for FY 2008-2013.

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.

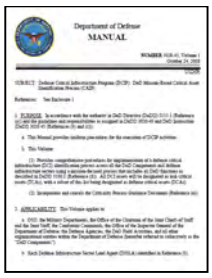


"Is the identified asset truly task critical or the only asset capable of performing a specific function that is critical to mission success?"

Critical Asset Identification Process – Execution System (CAIP-ES)

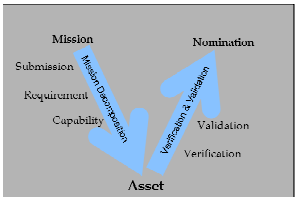
by Naval Surface Warfare Center Dahlgren Division Mission Assurance Division

The Critical Asset Identification Process (CAIP) was outlined to provide comprehensive procedures for the identification of Task Critical Assets (TCAs) for the Defense Critical Infrastructure Program (DCIP) using a mission-focused process. Past practices of identifying TCAs by Department of Defense (DoD) Components, defense infrastructure sectors and Military Departments (MILDEP) were many times incomplete and inconsistent.


Department of Defense
MANUAL

As TCAs were nominated, questions arose over validity from a variety of sources. Geographic Combatant Commands, Asset owners, Defense Infrastructure Sector Lead Agencies (DISLAs) would question the inclusion of an asset within their Area of Responsibility (AOR) or under their purview without their input. Missions are impacted by infrastructure in numerous ways, and often manifest interdependencies, and many times it is difficult to ascertain the true measure of an asset. Is the identified asset truly task critical or the only asset capable of performing a specific function that is critical to mission success?

The CAIP Execution System (CAIP-ES) is being created by the Mission Assurance Division at NSWC Dahlgren Division to provide stakeholders and decision makers with a consistent and repeatable process to successfully identify, nominate and validate TCAs. The system utilizes Microsoft Office Sharepoint Services (MOSS) 2007 to create a customizable collaborative environment to execute the CAIP. The Execution System incorporates the CAIP as the basis for TCA identification while augmenting the process with checks and balances designed to include the entire community. Users are provided a workspace on the CAIP for both internal and external collaboration. A host of capabilities are provided including the ability to invite other stakeholders into a documented discussion, sharing documents and information, and tracking the progress of a CAIP element.



As outlined in the CAIP, the process begins with Mission Decomposition. Each mission is broken down into SubMissions, with each SubMission broken into Requirements. Each Requirement is then broken down into Capabilities which may lead to a single asset meeting a Capability's Standards and Conditions. Once an Asset is identified by the Mission Owner and the Requirement Owner and the Submission owner verify and validate it as a single point of service, the Mission Owner can then chose to nominate the asset as a TCA. Throughout the process owners can invite others in the community into documented discussions. The process is applicable to DoD Components, defense infrastructure sectors and MILDEPs.

The CAIP-ES is currently undergoing final testing on the Mission Decomposition steps associated with the process while the Verification and Validation steps are in their design phase. Items of consideration include the Mission Owner's ability to assign the review of a Verified and Validated asset to an entity such as a DISLA or MILDEP, for a limited time period prior to final Nomination as a TCA.

The CAIP and CAIP-ES have one important requirement, the need for the entire community to participate. Without full participation from the DCIP community, a thorough, consistent, unified and reliable set of TCAs cannot be accomplished regardless of the tool used.

The CAIP is outlined in DoD Manual 3020.45-VI dated October 24, 2008.

How-To Register:

To register for access to the CAIP-ES users will be required to submit a User Access Request Form. Access is currently limited to three (3) per CIP entity (COCOM, Subordinate Command, Defense Sector Lead Agent, etc).

Entities are limited to three personnel because of additional costs incurred if membership exceeds a specific number. Organizations are responsible for tracking their own membership, removing personnel who depart, and replacing as required. The Access Request Form can be obtained from:

Kenneth C. Wallace, Mission Assurance Division
Phone: 540.653.0078, DSN: 249-0078, Fax: 540.653.4977
NIPR: Kenneth.C.Wallace@navy.mil, SIPR: Kenneth.C.Wallace@navy.smil.mil

"The CAIP added criteria addressing networked assets that must all be available to provide required capabilities, and caused DLA leaders to seriously assess whether the two sites should be classified as TCAs."

A DCIP Success Story

by Richard Hilliker, Defense Logistics Agency

Under the oversight of the DoD Logistics Defense Critical Infrastructure Program (DCIP) manager within the Defense Logistics Agency's (DLA) Logistics, Operations and Readiness directorate, multiple elements of DLA collaborated to implement a near "textbook" execution of the DCIP risk management concept for two DLA mission-critical infrastructure assets.

Following the guidance of DCIP directives issued since 2008, the assets were identified as critical by the mission owner, U.S. Northern Command. A DCIP risk assessment was then conducted by a combined team from the Defense Threat Reduction Agency (DTRA) and DLA Enterprise Support, and a risk management plan was developed by the asset owner, the DLA director of Information Operations. The director of Information Operations and the DLA Comptroller resourced the risk management plan, and the Information Operations directorate implemented actions that significantly reduced the risk of infrastructure failure to the warfighter. The entire process took about a year, and its success has been praised by the director of DCIP and the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs [ASD(HD&ASA)] as a prime example of how the DCIP risk management process should work.

The DLA assets involved were two dedicated operating centers supporting a key DLA cyber system. The system had never suffered a service disruption; therefore, the sites were presumed not to be Task Critical Assets (TCA) -- assets of such importance to operations in peace, crisis and war that their incapacitation would have a very serious, debilitating effect on the ability of DoD to fulfill its mission. However, in October 2008, the DCIP Critical Asset Identification Process (CAIP) directive established DoD-wide critical asset identification criteria. The CAIP added criteria addressing networked assets that must all be available to provide required capabilities, and caused DLA leaders to seriously assess whether the two sites should be classified as TCAs.

NORTHCOM nominated the DLA sites as TCAs, and one of them was added to the Joint Staff DCIP assessment schedule. A DCIP assessment process mission statement for the DLA site was drafted, noting that if one site was incapacitated, the cyber system capability would be switched to its back-up site, with personnel relocating to that site. The program manager for the asset also noted that current processing capability at each site was not able to sustain the full workload for both sites 24/7 without degradation of processing times, because redundant infrastructure and processing capability did not exist.

The February 2009 DCIP assessment of the site was modified to add a specific assessment of processing capability redundancy. The assessment report confirmed that redundant capabilities did not exist and offered a solution for the deficiency. The DLA Information Operations directorate worked with the DLA Comptroller to resource and implement risk management actions that significantly reduced the risk of infrastructure failure to the warfighter. The Logistics Sector DCIP program manager notified NORTHCOM of asset risk management status, and the two sites were removed from the DoD Task Critical Asset list.

In January 2010, after the risk management process was complete, DLA shifted one location's transaction processing to the other location due to a real world issue. All workload moved to the alternate location was processed without any delay or backlog, proving that the solutions implemented due to the risk

"...the instruction will require geographic COCOM intelligence components to provide the DCIP community with theater-level, AOR-specific threat assessments."

Intelligence Support to DCIP

by The Intelligence Sector

One of the most significant historical gaps in the DCIP community is the lack of specific and timely threat information to assess risks to critical infrastructure. As a risk management program, the DCIP is not effective in understanding risk unless all organizations have access to pertinent threat and hazard information. In many cases, threats to critical infrastructure may not be apparent in the course of routine intelligence analysis. In fact, the Intelligence Community (IC) may not be actively identifying, disseminating, and coordinating intelligence throughout DoD on a threat capability or intent to specific infrastructures because the Community may be unaware of nominated critical DoD assets and systems. Harnessing the full capabilities of the IC will enhance the accuracy of DCIP risk assessments.

Recognizing the need to improve intelligence support, the Intelligence Sector DISLA has undertaken a multi-pronged effort in support of the DCIP. This support includes strategic national assessments, coordination of regional threat and hazard assessments, and ad hoc intelligence production for analysis of threats to critical infrastructure. Each of these efforts directly complements the DoD Manual on Enhanced Threat and Hazard Assessments (ETHA).

The first step in this process is the formal tasking for support and coordination with all IC members, including service and Combatant Command (COCOM) intelligence components and national-level intelligence agencies. The Intelligence Sector has drafted an Instruction covering the IC's support to Defense Critical Infrastructure. This Intelligence Support policy will be issued by the Undersecretary of Defense for Intelligence. The basic foundation of this intelligence support is the development of a triennial strategic global assessment of threats to critical infrastructure. The first such triennial assessment was completed in 2009. Additionally, the instruction will require geographic COCOM intelligence components to provide the DCIP community with theater-level, AOR-specific threat assessments. These regional assessments will assist asset owners in conducting their site specific assessments under the ETHA guidelines.

Finally, the intelligence support policy establishes an Intelligence Support to DCIP working group chaired by the Chief Infrastructure Assurance Officer (CIAO) for the Intelligence Sector. The CIAO is a senior-level leader from Defense Intelligence Agency (DIA) who administers the Intelligence Sector and oversees all DoD intelligence provided to the DCIP. This working group will address the particular intelligence needs of the DCIP Community and ensure adequate support. When necessary, the working group will cooperate with national agencies to request additional specific intelligence collection and intelligence production in support of the DCIP Community's needs.

The Intelligence Sector has already increased intelligence support to the DCIP through several projects in response to urgent overseas critical asset analysis. A pilot project to assess vulnerabilities at overseas facilities through the use of intelligence analysis proved the viability of this capability. The success of this pilot project will lead to continued collaboration between the IC and the DCIP Community. The Intelligence Sector is continuing to work with OASD(HD&ASA) Defense Critical Infrastructure Office (DCIO) to enhance this relationship and initiate the Intelligence Support to DCIP working group. This effort will ultimately involve all members of the DCIP community and will provide support to all DoD components in assuring critical assets.

USEUCOM Participates in NATO BELCOAST 09

by John Taylor *with additional comments from the KDAS Team Joe Kammerman and Don Dudenhoeffer*

October 6-15, 2009, USEUCOM representatives Mr. John Taylor and Mr. Jared Irish from the Command's Defense Critical Infrastructure Program (DCIP) Office, participated in the NATO BELCOAST 09 Technology Demonstration Event at the Belgian Koksijde Airbase. The purpose of the BELCOAST was to provide the more than 20 participating vendors a venue to demonstrate their Critical Infrastructure Protection (CIP), intrusion detection, and surveillance systems. The event also provided opportunities for vendor systems' CIP and Anti-Terrorism/Force Protection (AT/FP) capabilities to be evaluated against eight different hostile-action scenarios

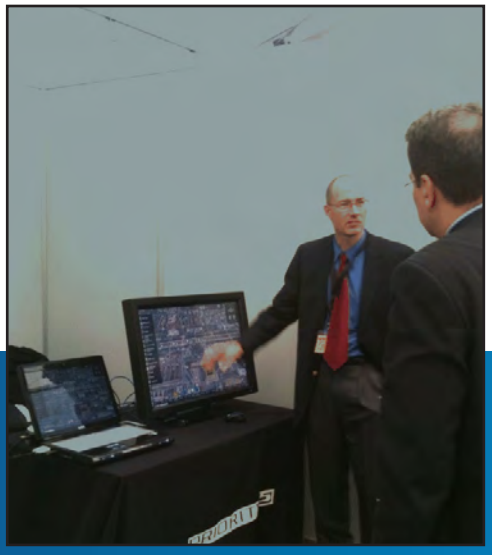
Unidentified Belgian military officers move between BELCOAST 09 demonstration sites on a closed runway at Koksijde Airbase, Belgium.

The USECUCOM participants, along with representatives from over 10 other NATO countries, performed as "technical experts" (TE's), observing and evaluating each of the vendors' systems in their ability to detect, recognize, and identify enemy forces, their intentions and actions. In addition, the TE's evaluated the vendors' systems on technical proficiency, ease of use, and ability to integrate with other systems existing force protection procedures.

The TE's received detailed briefings regarding each of the technologies provided by the many vendors and NATO military organizations. The observations and evaluations of the technologies took place during simulated, active enemy-action scenarios, as opposed to purely static displays. For instance, the scenarios simulated attacks on NATO critical infrastructure during both day and night conditions. The scenarios also included attempts to enter the base via a sewage pipe; a sniper attack on the base; attempted covert base intrusions by unidentified forces on foot; unidentified vehicles approaching the base; and an unidentified helicopter flying over the base.

The USEUCOM participants were able to meet with and exchange ideas with NATO personnel concerning DCIP and AT/FP policies and capabilities, as well as overall asset protection measures. This type of data exchange and cooperation will continue to prove invaluable as USEUCOM and NATO continue to mature their CIP/DCIP and AT/FP programs. Technology and information sharing with our NATO partners is highly beneficial to ensuring our DoD Critical Infrastructure Program maintains interoperability with NATO and other international partners.

The demonstration event went well and was a valuable tool for USEUCOM personnel to learn the current NATO "state of the art" in Critical Infrastructure Protection and Base Defense. USEUCOM DCIP successfully met new contacts and cultivated old relationships with NATO CIP personnel. .



Mr. Donald Dudenhoeffer, a member of the OASD (HD & ASA) exhibit team, demonstrates the Knowledge Display and Aggregation System to BELCOAST 09 attendees.

Department of Defense, Department of Homeland Security and Department of Justice Cosponsor the Technologies for Critical Incidence Response Conference (TCIP) for First Responders

by John Downey (DCIO)

Attendees view a demonstration of DoD's Knowledge Display and Aggregation System at the Technologies for Critical Incident Preparedness conference and exposition.

Arlington, VA -- The 11th Annual TCIP & Exposition hosted on February 2-4, 2010, at the Philadelphia Marriott Downtown, provided the DOJ, DHS, and DoD the opportunity to highlight the technologies, RDT&E investments, and training tools currently available and being developed for the emergency responder community, as well as provided a forum for emergency responders to discuss best practices and exchange information.

With 1,500 attendees and 150 exhibits and demonstrations, this conference offered a unique opportunity for emergency responders, business and industry, academia, and local, tribal, state, and federal stakeholders to network, exchange ideas, and address common critical incident technology, preparedness, response and recovery needs, protocols, and solutions.

The Office of the Assistant Secretary of Defense (Homeland Defense and America's Security Affairs) [OASD(HD&ASA)] was DoD's sponsoring agency, highlighting the Defense Critical Infrastructure Protection (DCIP) program and the department's "Section 1401" technology transfer program. The Deputy Assistant Secretary of Defense, Ms. Theresa Whelan, also provided one of the keynote addresses of the conference, speaking on the Department's role in supporting first responders in the homeland defense mission space.

Exhibits included displays covering DoD's responsibilities and efforts relating to the critical infrastructure protection program, situational awareness and common operating picture tools, and defense transfers of technology items and equipment in support of homeland security to Federal, State, and local first responders.

Named after the section of law from the Defense Authorization Act of 2003, The "Section 1401" program has six principal functions:

1. ***Identify*** technology items and equipment that have the potential to enhance public safety and improve homeland security;

2. ***Evaluate*** whether such technology items and equipment would be useful to first responders;

3. ***Facilitate*** the timely transfer;

4. I***dentify*** and eliminate redundant and unnecessary research efforts

5. ***Expedite*** the advancement of high priority Department of Defense projects

6. ***Communicate*** with first responders and facilitate awareness of available technology items and equipment to support responses to crises."

The conference exhibit served as a focal point for federal, state, local, and tribal first responders to learn firsthand the benefits to be derived from the program.

The solution involves the use of advanced visualization techniques, and incorporates a touch assisted command and control technology, i.e., "Touch Table", with critical infrastructure modeling capabilities developed by Idaho National Laboratory to create a framework for infrastructure interdependency modeling and analysis. Asset data from both proprietary and public domain databases is integrated and displayed, to fully model any potential or real national emergency. The resulting capabilities provide users with a methodology to assess the impact of natural disasters and terrorist events on the viability of key assets. The system provides users with a way to perform near real-time updates to readiness assessments as conditions change. The hands-on graphical interface combined with the overlay of actual asset data, gives emergency planners and first responders a tool to understand the progression and recovery actions necessary for a variety of events.

Used in the Global Situational Awareness Facility (GSAF) in the Pentagon, KDAS provides senior DoD leaders and action officers a common operational picture promoting situational awareness for real-time emergencies and a platform for conducting modeling and simulation exercises. Modeling functions include analysis of impacts on critical civilian and military infrastructure assets such as electrical distribution and mass transit and any cascading effects those disruptions may have on other assets. Simulations on civilian and VIP evacuations of congested metropolitan areas can also be accomplished using real world or simulated impediments to traffic flow.

USPACOM CIP Risk Management Strategy Event Timeline

by MAJ N. Isaac Cavazos, Dave Hazlett, Brian McKay (USPACOM J345, Critical Infrastructure Protection)

In September 2009, USPACOM embarked on a new approach to manage risk to its task critical assets (TCA) and enable informed risk decision-making. The J34 developed a 34-month CIP event timeline to execute its CIP risk management strategy. As DoD guidance evolved and CIP program management activities became more complex and interdependent, a strategic view was obviously called for. The goals of the strategy include the following:

- Revalidating and nominating new TCAs, to refresh and update baseline elements of information (BEI)• Conducting full risk assessments (including threat, hazard, and vulnerability assessments and remediation planning) for all TCAs
- Delivering risk decision packages for all Tier TCAs for the USPACOM Operations Director's (J3) approval
- Providing validated lists of TCAs to the Joint Staff for DCA consideration

Approach to Conducting Critical Asset Assessments

USPACOM developed a rolling, three-year CIP event timeline to refresh TCA risk management activities. The USPACOM J34 will use the information from each phase activity to complete the subsequent phases. The timeline follows the standard sequence of events outlined in DODI 3020.45 for DCIP Management with some modifications for theater review. Time durations for each phase are prescribed in some cases, and in other cases are based on best-guess estimations by the J34 CIP staff. Table 1 summarizes the phases and time periods of performance.

Phase	Time
Critical Asset Identification Process (CAIP)	2 months
Threat/Hazard Assessment	1 month
Vulnerability Assessment	2 months
Risk Assessment	3 months
Remediation Planning	4 months
Impact Assessment	1 month
Risk Decision Package (RDP) Preparation	1 month

Table 1: Phases of CIP Event Timeline and Period of Performance

The event timeline starts with the identification of critical assets by service components in coordination with installation level asset owners. Sector leads must identify and nominate any potential TCAs that are not DoD-owned, including assets owned by other government agencies, commercial assets, and foreign-owned assets. Service components conduct appropriate steps of the CAIP (from DODM 3020.45 V1) to nominate TCAs that are critical for their mission essential tasks (MET). The component TCA nominations are then submitted to the USPACOM sector leads for validation. The sector lead validation evaluates nominated TCAs against other sector assets and capabilities to ensure we have identified only the assets that are critical to the COCOM mission.

Following the TCA validation, component representatives and sector leads continue with the threat, hazard, and vulnerability assessments for their Tier 1 and 2 TCAs, focusing the vulnerability assessments on the TCAs with threat/hazard assessment scores of 8 or above. Although the ETHA Manual was not yet published when the Risk Management Strategy began, USPACOM elected to adopt its methodology. Upon completion, the service components and sector leads complete the risk assessment and remediation planning steps. USPACOM J34 staff members assist the asset owners and sector leads by completing the impact determination for Tier 1 assets and developing the risk decision packages (RDP) for all Tier 1 TCAs.

In order to accommodate the resource constraints across the theater and to meet Joint Staff and OASD(HD&ASA) priorities, USPACOM divided the overall timeline into 6 geographic regions. The separation of regions also takes into account the overall number and significance of the current TCAs. USPACOM is executing the 14 month assessments according to the schedule in Figure 1, and is currently midway through Region 1 and in the third month of the Region 2

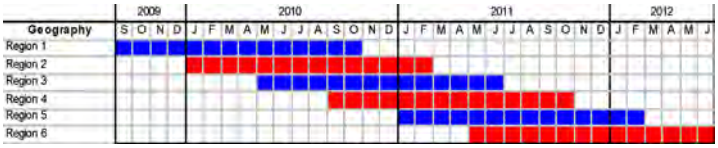


Figure 1: USPACOM Risk Management Strategy Schedule

Challenges with the Strategy and Opportunities for Improvement

The largest challenges as USPACOM has started the initial phases of this strategy involve the non-DoD-owned assets and the amount of responsibility placed on USPACOM sector leads (represented by various headquarters directorates). The event timeline calls for the service components and sector leads to perform the CAIP, threat/hazard assessment, vulnerability assessment, risk assessment, and remediation planning for non-DoD-owned assets. These activities have been difficult not only due to the limited CIP resources but also the lack of visibility the sector leads and components have on non-DoD-owned assets. USPACOM has engaged its sector leads to assist them with initial training and orientation sessions, as well as continued support during each phase to help guide the sector leads on how to conduct different phases of the strategy.

Non-DoD-owned assets pose significant challenges in both the assessments and remediation actions for critical assets. Without established relationships and agreements, it will remain difficult for sector leads and the USPACOM J34 staff to effectively reduce residual risk associated with non-DoD-owned assets. Difficulties are further compounded for non-DoD-owned TCAs outside the United States and its territories that USPACOM relies on to accomplish its missions.

Another challenge with the Risk Management Strategy implementation has been the lack of CIP expertise at the installation/asset owner levels. USPACOM and its components rely on asset-level POCs to provide BEI data, localize threat/hazard and vulnerability assessments, identify remediation options, and implement risk response activities. For the most part, the POCs have no CIP training or formal program responsibilities. Consequently, USPACOM and its components have to employ work-arounds such as planning ad-hoc training sessions, or conducting multiple staff assistance visits.

The USPACOM J34, components and sector leads have been meeting for in-progress reviews on a monthly basis to discuss the status and challenges for each phase of the strategy, as well as to identify lessons learned for the next region. The group has applied lessons from the first 6 months of the process to modify the approach for future evaluations, with the ultimate goal of producing a refined assessment process to identify and validate all theater TCAs, and provide USPACOM leadership with the opportunity to make informed risk decisions at the conclusion of each phase of the 34-month timeline.

CIP Related Conference Schedule

-

AFRICOM AT/CIP Conference
3-6 May, Germany

-

FL Governor's Hurricane Conference
26-28 May, Orlando, FL

-

AF CARM Program Working Group
19-22 July, Herndon, VA

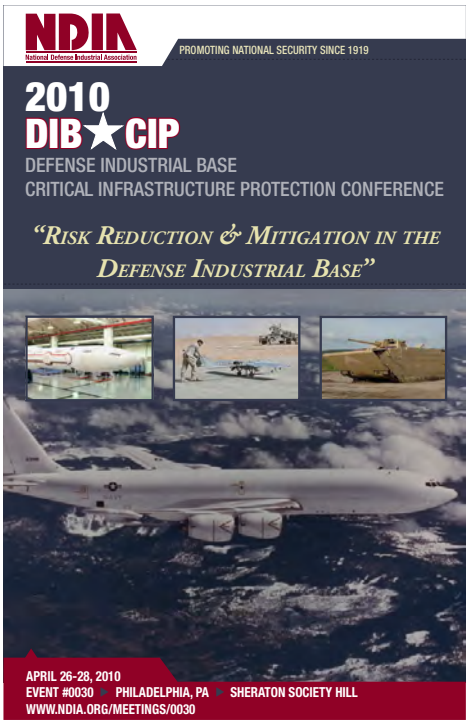
Need Access to the DCIP Web Portal?

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.

2010 DIB CIP - DEFENSE INDUSTRIAL BASE CRITICAL INFRASTRUCTURE PROTECTION CONFERENCE

"Risk Reduction & Mitigation in the Defense Industrial Base"

http://www.ndia.org/meetings/0030 <http://www.ndia.org/meetings/0030>



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