THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 8

FEBRUARY 2007

DEFENSE INDUSTRIAL BASE

Contact: CIPP01@gmu.edu

703.993.4840

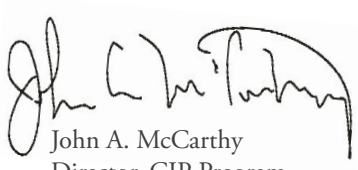
Click **here** to subscribe. Visit us online for this and other issues at http://cipp.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Many previous issues of *The CIP Report* have focused on the Department of Homeland Security's role in protecting critical infrastructure, but rarely have we had the opportunity to highlight the role of the Department of Defense in the protection of critical infrastructure and key resources (CI/KR). The Department of Defense (DoD) is the Sector Specific Agency responsible for the Defense Industrial Base, a sector that has the capabilities to perform research and development, design, produce, deliver, and maintain military weapon systems, subsystems, components and parts to meet military requirements. Furthermore, the DoD is responsible for ensuring that the defense critical infrastructure is available to the war fighter, a responsibility we can currently see enacted real-time in Iraq.

This month's issue of *The CIP Report* features a series of articles provided to us by the Office of the Assistant Secretary of Defense. An interview of William Bryan, the Director of the Defense Critical Infrastructure Protection Office of the Assistant Secretary of Defense conducted by the CIP Program Law Team, identifies the mission and capabilities of the DoD in the critical infrastructure arena, as well as the relationships between DoD, the Department of Homeland Security and the private sector. The interview also explores some of the challenges faced by the DoD. In addition to this informative article, we also include an extensive overview of the Defense Industrial Base's (DIB) Sector Specific Plan, which is required by each Sector Specific Agency- in this sector, the DoD. Finally, Assistant Secretary of Defense, Peter F. Verga, provides an overview of Defense Critical Infrastructure.

We are very pleased to be able to feature the Defense Industrial sector, and we are particularly grateful to all of the individuals in the Department of Defense that provided us these insightful articles and interviews that highlight the critical mission of the DoD in critical infrastructure protection.



John A. McCarthy
Director, CIP Program
George Mason University, School of Law

Interview with William Bryan, Director Defense Critical Infrastructure Protection Office of the Assistant Secretary of Defense

The CIP Law Team conducted an interview with Mr. William Bryan, Director, Defense Critical Infrastructure Protection (CIP), Office of the Assistant Secretary of Defense (Homeland Defense).

What are the key distinctions between the roles of the Department of Defense (DoD) and the Department of Homeland Security (DHS) in critical infrastructure protection (CIP)?

Mr. Bryan: Scope and mission focus are key distinctions. DHS is responsible for safeguarding critical infrastructure (CI) by identifying and protecting all assets that are designated as such. DoD supports this effort, so it is vital that DoD understand CI vulnerabilities and how DHS will address them.

For DHS, essentially there is a list of critical assets that must be protected at all times. For DoD, there is more of a time and scenario-specific dimension. DoD must be able to assure that defense missions can be carried out, and therefore the supporting infrastructure is resilient and available. For example, national ports are considered CI by DHS. Yet for DoD, which port and when are the crucial elements. If the DoD must carry out an overseas mission, the port relevant to that mission, and the time it is needed, will define its CIP status.

For DHS, public opinion and confidence are very important issues and therefore must be kept in mind as DHS works to protect CI. For DoD, the overriding issue is the ability to deploy and sustain military operations abroad. Time and scenario do not determine criticality but rather define the priority of that asset at that moment. In the end what evolves is a partnership in which timing, scope, and mission-specific variables are the focus for DoD as it defines its CI.

DoD has a unique history and scope of capabilities. What are the ways the DoD can contribute to CIP as a result of these capabilities?

Mr. Bryan: DoD contributes to CIP in the policy arena as well as operationally. Within DoD, there are ten distinct critical infrastructure sectors. DoD writes CIP policy for all of these sectors. DoD is the Sector Specific Agency (SSA) responsible for the Defense Industrial Base (DIB). The DIB is the DoD, U.S. Government, and private sector worldwide industrial complex with capabilities to research and develop, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Through industry partnerships, DoD works to execute policy related to this sector. Both writing policies as well as executing DIB SSA responsibilities require detailed knowledge of commercial infrastructure dependencies and vulnerabilities.

Operationally, DoD has a strong science and engineering base, with perhaps some of the best infrastructure engineers in the country. In the same manner as we analyze foreign infrastructure in support of our deployed forces, we have applied similar processes and techniques in defense of the homeland. These techniques and skill sets can be used to identify domestic vulnerabilities and thereby indicate where steps need to be taken to strengthen domestic CI. Once we know the weakness, we can better design a strong defense or a more resilient infrastructure. DoD has a long history of this kind of in-depth analy-

(Continued on Page 3)

"For DHS, essentially there is a list of critical assets that must be protected at all times. For DoD, there is more of a time and scenario-specific dimension. DoD must be able to assure that defense missions can be carried out, and therefore the supporting infrastructure is resilient and available."

Bryan Interview *(Continued from Page 2)*
sis, both of critical industrial as well as government assets. I think DoD can be a very important contributor to this kind of analysis and perhaps even assist to create a single source of vetted data to which all agencies have access. Having such a single source will add to the efficiency of the government's efforts in mitigating CI vulnerabilities.

DoD has been particularly successful with respect to the establishment of benchmarks and training for the assessment of CI vulnerabilities. DoD, through the efforts of the Mission Assurance Division (MAD), Naval Surface Warfare Center (NSWC), Dahlgren, VA, has created a curriculum for training CIP assessors which is now being employed by the West Virginia National Guard in Camp Dawson, WV. There has been interagency and even industry interest in our assessment work as well. However, it should be noted that these assessments are not your traditional "anti-terrorism or force protection" assessments. We are pursuing a holistic approach incorporating the assessment of human, physical and cyber components of the DIB, currently named the CIP-Mission Assurance Assessment (CIP-MAA). We are achieving that objective.

DoD has undertaken significant work developing assessment techniques and models as well as, through its curriculum, standardized CI-related assessments. This unique capability can be a useful tool for all those working to identify and remediate vulnerabilities to our CI.

What are the major impediments to a larger role for DoD in CIP?

William (Bill) Bryan is the Director for CIP and leads all CIP and Defense Industrial Base (DIB)-related activities within the Office of the Assistant Secretary of Defense for Homeland Defense (OASD (HD)). He advises key DOD leadership on the relevance of current CIP and DIB capabilities, methodologies and technologies in support of military and civil homeland defense efforts. CIP focuses on the identification, assessment, and security enhancement of physical and cyber assets and associated infrastructures essential to the execution of the National Military Strategy to include the assurance of the most critical defense industrial base assets. In the course of these duties, Mr. Bryan Interfaces with the Homeland Security Council, National Security Council and other federal agencies regarding the leveraging of DOD CIP capabilities in support of the National Strategy for Homeland Security. Mr. Bryan currently serves in the Virginia Army National Guard.

Mr. Bryan: Although each organization is responsible for articulating their resource requirements, competing priorities and authorities often scope CIP activities within the department. While DoD Directive 3020.40, "Defense Critical Infrastructure Program" (DCIP), defines the roles and responsibilities for CIP within and across the DoD, organizational requirements compete for the same pool of resources. It is for this reason that we have to be diligent in leveraging the activities of others in the interagency arena so we can better focus our resources to eliminate redundancy.

Another significant impediment relates to our work globally. We are involved in international efforts to coordinate CIP. How this is done will vary depending upon the most effective type of relationship we maintain with a given country. For example, in some cases military to military relations are excellent and the best vehicle for CIP-related communication and collaboration is through the Combatant Command responsible for that part of the world. In other cases, diplomatic channels are more effective and we seek assistance from the Department of State in these instances. DoD's key role is to support the war-fighting Commanders and enable their successful execution of the national military strategy.

How would you describe the relationship between DoD and DHS regarding CIP?

Mr. Bryan: It is a growing relationship. The National Infrastructure Protection Plan (NIPP) orchestrates how we communicate, both in times of crisis and during peacetime. I have found DHS to be very responsive to our input. Additionally, DoD was able to have a strong impact on the creation of the NIPP. DoD offered substantive comments which were adopted by DHS when putting together the final NIPP document. DHS has shown itself to be receptive to change even while challenged to bring a structured approach to this complex problem.

Does DoD CIP have a strong relationship with the private sector?

Mr. Bryan: I first want to say that *(Continued on Page 9)*

The Defense Industrial Base

Introduction

The Department of Defense (DoD) is executing the Strategy for Homeland Defense and Civil Support that builds upon the concept of an active, layered defense called for in the United States National Defense Strategy. Near the core of this defense lie the critical infrastructure and key resources (CI/KR) of the United States essential to the Nation's security, economic vitality, and way of life.

The Secretary of Homeland Security, in coordination with the heads of all cabinet level agencies, published the National Infrastructure Protection Plan (NIPP) in June 2006. The NIPP provides the framework for the unprecedented cooperation that is essential to develop, implement, and maintain a coordinated national effort that brings together all levels of government, the private sector, and international organizations and allies. An essential element of this framework is the complementary Sector Specific Plans (SSP) required of each of the Sector Specific Agency (SSAs). The Department of Defense is the SSA for the Defense Industrial Base (DIB) and therefore responsible for the DIB plan to implement the NIPP. More specifically, the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, Defense Critical Infrastructure Program (OASD(HD&ASA)/DCIP) is responsible for leading this effort. The DIB SSP supports the planning assumptions outlined in the NIPP as well as DIB sector-specific planning assumptions relevant to the assurance of the DIB.

The DIB is the DoD, U.S. government, and private-sector worldwide industrial complex with capabilities to perform research and development, design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other Federal Departments and Agencies. Defense-related products and services provided by the DIB equip, inform, mobilize, deploy, and sustain forces conducting military operations world-wide. Because only a small fraction of DIB facilities are DoD-owned, the DIB SSP is focused on government and private sector actions that can support private owner/operator efforts at DIB facilities determined to be critical to national security.

"The DIB includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other Federal Departments and Agencies."

Sector Security Partnership Framework

Within the Department of Defense, there are several key players in the execution of the NIPP and the DIB SSP. The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, in full coordination with the OASD(HD&ASA), oversees the processes necessary to develop and prioritize the DIB critical asset list. The Defense Contract Management Agency (DCMA) is responsible for executing the day-to-day activities of the sector.

Under the security partnership framework established in the NIPP, the principal coordinating bodies within the DIB sector are the DIB Government Coordinating Council (GCC), DIB Sector Coordinating Council (SCC) and the Critical Infrastructure Protection Advisory Council (CIPAC).

The DIB GCC seeks to provide effective coordination of DIB sector security strategies and activities, policy, and communication across government. In addition, the GCC coordinates with the other government sector-specific agencies that interact with the nation's DIB. The DIB Sector Coordinating Council (SCC) was established as the private sector counterpart to the GCC to enable private sector owners and operators to coordinate among themselves on sector initiatives, including response and recovery. It further provides a recurring forum for the DIB owners/operators to facilitate information sharing, identify common areas of interest, leverage activities, illuminate duplicative processes, and develop a prioritized list, by function area,

(Continued on Page 5)

DIB *(Continued from Page 4)*
of required DIB CIP program improvements. The DIB SCC is an independent, self-governed body organized by the owners and operators of the DIB.

The CIPAC was established as the framework to enable private sector owners and operators to engage DoD, the Department of Homeland Security (DHS), and other Federal departments and agencies on homeland security issues. The CIPAC is a Federal Advisory Committee Act exempt body pursuant to section 871 of the Homeland Security Act.

Risk Management Framework

DoD has an aggressive program aimed at assessing the components of risk to critical DIB assets. Prior to the issuance of Homeland Security Presidential Directive 7 (HSPD-7) and current NIPP guidance, DoD's DIB program was primarily focused on assessing and mitigating risk to DIB assets critical to accomplishing DoD missions. DoD has since embraced the broader focus and emphasis on impacts to areas other than mission accomplishment.

When assessing DIB assets, DoD evaluates individual facilities rather than entire companies because a single company may own both critical and non-critical DIB assets. The DIB is best characterized as a loose federation of assets where impacts of loss or damage tend to be discrete. The risk assessment process for critical DIB assets consists of an evaluation of factors that may cause the direct, indirect, temporary, or permanent loss or degradation of critical materials and services. The evaluation includes the following:

- Industrial and business analysis that defines the business, economic, technology, and production risks that may affect adversely the capacity of the supplier to provide the critical material or service;

"The DIB is best characterized as a loose federation of assets where impacts of loss or damage tend to be discrete. The risk assessment process for critical DIB assets consists of an evaluation of factors that may cause the direct, indirect, temporary, or permanent loss or degradation of critical materials and services."

- Common commercial infrastructure analysis that maps critical supplier dependencies and interdependencies with the supporting commercial infrastructure sources (e.g., energy, telecommunications, transportation) to identify single or otherwise significant points of failure, potential remediation actions, and resolution, where viable, through the responsible Federal Departments and Agencies;

- Predictive analysis processes that help to define or suggest the existence of a problem for a critical supplier before it would otherwise be known;
- Vulnerability assessments that define the vulnerabilities of the supplier, identify impact if lost, propose and rank countermeasures, and include a variety of assessment means and tools for use by the facility and the government for early identification, evaluation and resolution of mission-impacting issues;

- Threat assessments for the full threat spectrum, from man-made threats including the intentions and actions of nation-states, national and transnational criminal entities, and terrorists to accidents and acts of nature.

Due to the large number of DIB assets, the voluntary nature of the private sector compliance, and the limited resources available to carry out comprehensive risk assessments, DoD must perform an initial screening. The screening assesses criticality, vulnerability and threat as well as potential consequences. HSPD-7 focuses on the identification, prioritization and coordination of protection of critical infrastructure. In addition, the NIPP tasks SSAs to consider four categories of consequences:

- Human Impact: Effect on human life and physical well-being (e.g., fatalities, injuries);

- Economic Impact: Direct and indirect effects on the economy (e.g., cost to rebuild the asset, costs to respond to and recover from attack, downstream costs resulting from the disruption of products or services, and long-term costs due to environmental damage);

(Continued on Page 12)

Developing Resiliency – An Overview of Defense Critical Infrastructure

Peter F. Verga, Assistant Secretary of Defense
Homeland Defense & Americas Security Affairs

Peter F. Verga

Introduction

The ability to assure the availability of critical infrastructure and key resources (CI/KR) of the United States is vital to our national security, public health and safety, economic vitality, and way of life. Terrorist attacks or catastrophic disasters that undermine CI/KR cannot only disrupt essential government missions, public services, and economic functions but could also have serious cascading effects that extend far beyond any immediate losses in human lives, property, and the economy.

The Department of Homeland Security (DHS) is responsible for assessing, securing, and protecting the key resources and critical infrastructure of the U.S. To do this, DHS works in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

The Department of Defense (DoD) is responsible for ensuring defense critical infrastructure (DCI) is available to the war fighter. DCI includes "DoD and non-DoD networked assets essential to project, support, and sustain military forces and operations worldwide" (DoD Directive 3020.40). Homeland Security Presidential Directive (HSPD)- 7 assigns DoD responsibility for identifying, prioritizing, assessing, providing remediation, and protecting defense critical infrastructure and key resources. In addition, HSPD-7 establishes DoD as the lead Sector-Specific Agency for the Defense Industrial Base, which is discussed further below.

National Critical Infrastructure

Prevention and Protection

As discussed in The Strategy for Homeland Defense and Civil Support, DoD is responsible for deterring and, when directed by the President, defeating direct attacks against the United States. The President or the Secretary of Defense may direct U.S. military forces to protect non-DoD assets of national significance that are so vital to the nation that their incapacitation could have a debilitating effect on the security of the U.S. For example, since 9/11, DoD, through Operation NOBLE EAGLE, has conducted air patrols to protect major U.S. population centers, critical infrastructure, and other sites. DoD also maintains Quick Reaction Forces and Rapid Reaction Forces, highly trained U.S. Army and U.S. Marine Corps units, ready to respond to a wide range of potential threats to the U.S. homeland, including critical infrastructure protection. In addition, in October of 2004, the Secretary of Defense was granted the authority to fund the Governor of a State's employment of his or her National Guard in homeland defense activities to protect critical infrastructure or assets if such infrastructure or assets are determined by the Secretary to be critical to national security.

Response and Recovery

At the direction of the President or the Secretary of Defense, the Department provides defense support to civil authorities in order to manage the consequences of an attack or a disaster. Civil authorities are most likely to request DoD support where we have unique capabilities to contribute or when civilian responders are overwhelmed. DoD's contributions to the comprehensive national response effort can be critical, particularly in the near-term, as DHS and other agencies strengthen their preparedness and response capabilities.

Defense Critical Infrastructure – The Need for Resiliency

To execute its missions in a global environment, DoD relies on a worldwide infrastructure to sustain all military bases of operation. As such, DoD needs to understand the

(Continued on Page 7)

Resiliency *(Continued from Page 6)*
risks to infrastructure globally upon which its missions rely. Defense Critical Infrastructure is composed of functional sectors that provide the operational and technical capabilities essential to mobilize, deploy, and sustain military operations in peacetime and war. These assets are owned or controlled by DoD, other U.S. governmental agencies, domestic and foreign private sectors, host-nation governments, third-nation governments, and multinational consortia.

When located on DoD installations, the installation commander or facility manager is responsible for identifying, prioritizing, and assessing the availability of that DCI. In some instances, however, DCI is located at public or private sites beyond the direct control of DoD. During these instances, DoD must work with the public or private sector owners, or, in the case of international DCI, with host nations to ensure the availability and survivability of the infrastructure DoD relies upon.

DCI crosses organizational and political boundaries, and is addressed in three broad categories:

- DoD-owned assets that support the National Military Strategy. This includes DoD assets worldwide for which DoD can take direct steps to manage risks to these assets.

- Non-DoD-owned assets that support the National Military Strategy. This includes other government-owned infrastructure, commercial-owned infrastructure, and the DIB. DoD must work collaboratively with those asset owners to encourage and facilitate the management of risks to these assets.

- Non-DoD-owned assets that are so vital to the nation that their incapacitation, exploitation, or destruction could have a debilitating effect on the security or economic well-being of the nation or could negatively affect national prestige, morale, and confidence. This includes key resources, national symbols and events, and potential targets that do not support DoD missions, but are crucial to U.S. security and its economic well-being. As directed by the President, DoD supports the Department of Homeland Security (DHS) in safeguarding these assets.

Assessing the risk and mitigating potential effects to DCI is essential to ensuring the mission readiness of our military forces to protect the United States and to project power globally. However, because resources are constrained, uniform security of all DCI is not possible. Instead, DoD prioritizes DCI and key assets based on their criticality to executing the National Defense Strategy and seeks to minimize their vulnerability with an integrated risk management approach. To this end, DoD has developed a Risk Management Strategy to:

- Identify infrastructure critical to the accomplishment of DoD missions, based on a mission area analysis.

- Assess the potential effect of a loss or degradation of critical infrastructure on DoD operations to determine specific vulnerabilities, especially from terrorist attack.

- Manage the risk of loss, degradation, or disruption of critical assets through remediation or mitigation efforts, such as changes in tactics, techniques, and procedures; minimizing single points of service; and creating appropriate redundancies, where feasible.

- Protect infrastructure at the direction of the President or the Secretary of Defense where the nature of the threat exceeds the capabilities of an asset owner and civilian law enforcement is insufficient.

- Enable real-time incident management operations by integrating current threat data and relevant critical infrastructure requirements.

The Assistant Secretary of Defense for Homeland Defense leads the effort to ensure resiliency across the DCI. To achieve this, the Assistant Secretary established the Defense Critical Infrastructure Program (DCIP) and published DoD Directive 3020.40, which set forth DCIP policy and responsibilities within the Department. Under this policy, the identification, prioritization, assessment, and assurance of DCI is managed as a comprehensive program that includes the development of adaptive plans and procedures to mitigate risk, restore capability in the event of loss or degradation, support incident management, and protect
(Continued on Page 8)

Resiliency *(Continued from Page 7)*
DCI related sensitive information. Through DCIP, DoD has developed a Risk Assessment Handbook which is a standardized "How To" manual for identifying, assessing, and mitigating critical assets within DoD. In addition, we conduct vulnerability assessments on our most critical assets. These structured processes help the various services (Army, Navy, Air Force, and Marine Corps), Combatant Commanders (responsible for commanding forces on the ground), and sector lead agencies identify and prioritize their critical infrastructure and assist the decision makers in managing risk.

Defense Industrial Base

Homeland Security Presidential Directive 7 (Critical Infrastructure Identification, Prioritization, and Protection), designated Federal agencies as Sector-Specific Agencies for critical infrastructure and key resource sectors such as information technology, telecommunications, chemical, transportation systems, banking and finance, public health, food and agriculture, and energy. As was mentioned above, DoD was designated the Sector-Specific Agency responsible for the Defense Industrial Base (DIB) sector. The Defense Industrial Base (DIB) is a worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapons systems, subsystems, components, or parts to meet military requirements. These defense-related products and services are essential to mobilize, deploy, and sustain military operations. The DIB consists of hundreds of thousands of sites, the majority of which are privately owned.

Under HSPD-7, as the Sector-Specific Agency for the DIB sector, DoD is responsible for:

- Collaborating with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;
- Conducting or facilitating vulnerability assessments of the sector; and,
- Encouraging risk management strategies to protect against and mitigate the effects of attacks or natural disasters which impact critical infrastructure and key resources.

With respect to support for the DIB, the Defense Contract Management Agency (DCMA), in coordination with the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, developed a process to identify critical DIB assets globally. DCMA is responsible for day-to-day DIB activities and oversees the process of identifying and prioritizing DIB assets.

DCMA conducts DIB Site Awareness Visits to reach out to our critical DIB sites. In addition, DCMA coordinates on-site assessments in conjunction with National Guard CIP Mission Assurance Assessment teams. These assessments seek to discover the vulnerabilities each DIB site faces in terms of various threat scenarios and their interdependencies with commercial infrastructure such as power and telecommunications. Given the number of DIB assets which are privately owned, this work requires significant coordination with, and support from, the private sector.

Conclusion

Today's challenges are daunting: transnational terrorists bent on killing innocent people, destroying our civilization, and pursuing weapons of mass destruction to inflict mass casualties; rogue states that have or are pursuing weapons of mass destruction; an interconnected, global information network that opens doors to unprecedented information sharing and vulnerabilities; and the devastating power of catastrophic disasters.

Despite these challenges, Americans depend on the Government everyday to ensure access to critical infrastructures they depend upon. A resilient U.S. infrastructure will not only make Americans more secure from terrorist attack, but will also reduce our vulnerability to natural disasters.

For its part, DoD will continue to identify, prioritize, assess, and assure the availability of DCI. This will support our readiness to defeat direct attacks against the U.S. homeland, project power globally, and assist DHS and other Federal, State, and local partners, as appropriate, in safeguarding our nation's citizens, territory, and critical infrastructure. ❖

Bryan Interview *(Continued from Page 3)*
we are fortunate to have not only the commitment from industry leaders, but from our senior DoD leaders as well, in executing our SSA responsibilities. We have long standing relationships with both our private sector (industry partners) and with key utility providers. The quality and nature of this relationship contributed to the successful stand-up of the DIB Sector Coordinating Council (SCC), as defined in the NIPP. The DIB SCC is comprised of key defense industry associations with plans to expand and have representation from small, medium and large companies. The SCC is organized, managed, and chartered by the sector itself and is currently chaired by Major General (retired) Barry Bates from the National Defense Industrial Association (NDIA).

As issues or concerns are identified by the SCC, or as vital sector information needs to be shared with government, these actions are raised to the DIB Government Coordinating Council (GCC) through the Critical Infrastructure Partnership Advisory Council (CIPAC) The strength of the GCC-SCC-CIPAC structure is that it enables the private sector to come to the government and tell us how best to support them as they work to help us. We, in turn, are then better able to provide and facilitate the services needed to maintain the viability of our DIB.

The DIB encompasses approximately 300,000 contractors. It is not practical or necessary to dedicate the same level of effort in addressing each site, so identifying our most critical sites is essential. Through a series of criteria developed by the Defense Contract Management Agency (DCMA)/Industrial Analysis Center (IAC), and approved by the Under Secretary of Defense for Acquisition, Technology and Logistics, we have identified our important capabilities and our most critical DIB assets. This breakdown enables the DoD to focus our limited resources on those sites having the greatest mission impact.

DoD is involved in facilitating and, in some cases, conducting CIP-MAAs at select DIB sites. As I mentioned earlier, DoD has developed DCIP assessment benchmarks and mission analysis tools which can be used by private sector entities to better address their CI needs and dependencies. We look to assist industry in integrating these processes into their business continuity and disaster recovery plans. We do this both by providing training and/or through site visits.

DoD is responsible for protecting "Defense Critical Infrastructure" (DCI). Who should define DCI? How broadly should it be defined? Is there non-DCI that the President may order military forces to protect?

Mr. Bryan: Defense Critical Infrastructure is defined in DoD Directive 3020.40 as:

> "DoD and non-DoD networked assets essential to project, support, and sustain military forces and operations worldwide."

Through a deliberative process we first answer the question "What is critical?"...followed by "Is it vulnerable?"...then finally "What can be done about it?" As discussed earlier, the "critical" designation is directly tied to the mission that asset supports coupled with the time and scenario the asset is utilized.

DCI can be viewed in three different categories; those owned by DoD, those influenced by DoD and those of interest to DoD. Protection responsibilities for those assets owned by DoD (i.e. military facilities) clearly fall upon DoD and more specifically the installation commander. For those sites with
(Continued on Page 10)

DoD Directive 3020.40 Definitions

Defense Critical Infrastructure: DoD and non-DoD networked assets essential to project, support, and sustain military forces and operations worldwide.

Mission Assurance: A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan… It links numerous risk management program activities and security related functions—such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—to create the synergistic affect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.

Bryan Interview *(Continued from Page 9)*
significant DoD influence (i.e. the Defense Industrial Base), protection responsibilities fall on the asset owners. However, due to the nature of the relationship and partnership with the DIB and DoD dependencies on what the DIB provides, DoD takes a very active role in ensuring the viability of our most critical DIB sites. Finally, there are sites that DoD does not own nor can they influence but there is interest (i.e. chemical storage facilities, dams, certain icons). Only under the most extreme circumstances and when directed by the President or Secretary of Defense will DoD deploy forces to protect them.

Mission Assurance is an important concept for DoD CIP. Could you please talk a little about Mission Assurance and its role within DoD CIP?

Mr. Bryan: The question would probably be better phrased as "What is the role of DoD CIP within the Mission Assurance framework?"

The Department of Defense Strategy for Homeland Defense and Civil Support (June 2005) sets forth the broad direction of homeland defense and civil support. In the Strategy, "achieving Mission Assurance" ranks third of five key objectives, defining Mission Assurance as "…the certainty that DoD components can perform assigned tasks or duties in accordance with the intended purpose or plan..."

The Strategy outlines five capabilities needed to achieve Mission Assurance:

- Force Protection
- Preparedness and Protection of Defense Critical Infrastructure
- Preparedness of the Defense Industrial Base
- Preparedness to Protect Designated National Critical Infrastructure
- Defense Crisis Management and DoD Continuity Preparedness

In a June 24, 2005 memorandum, the Deputy Secretary of Defense recognized Mission Assurance as one of ten DoD activities necessary to implement the Strategy.

In addition, DoD Directive 3020.40, further defines Mission Assurance as:

> "A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan… It links numerous risk management program activities and security related functions—such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—to create the synergistic affect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations."

Mission Assurance (MA) is a critical component in the active, layered defense concept established in the National Defense Strategy, ranging from global access and power projection to installation preparedness and security. Mission Assurance is achieved when DoD Components, acting alone or in concert, can successfully execute their responsibilities to perform DoD Mission Essential Functions.

Finally, what role does the National Guard play in DoD CIP?

Mr. Bryan: I think the National Guard has a significant role to play in CIP.

A good example of a role the National Guard plays in DoD CIP is in the area of assessments. We have found that in looking at individual companies within the DIB, a "one-size-fits-all" approach to assessments just doesn't work. Companies must answer to shareholders and operate in very different environments from state to state and region to region. What is needed to adequately address the specific situation of various DIB companies is a tailored approach to each assessment. Here we have found the National Guard to be particularly adept.

In collaboration with the DCMA, the National Guard Bureau, the West Virginia National Guard, and the Mission Assurance Division/NSWC, we have developed the CIP-MAA curriculum and the infrastructure to train assessors to a given standard. The CIP-MAAs have proven to be very flexible. Furthermore, companies have welcomed the National Guard to their site and have demonstrated cooperation in assessment activities. This partnership with industry is essential in our efforts to "help industry, help us."

We were pleased recently when the Joint Requirement Oversight Council (JROC) looked at our *(Continued on Page 13)*

The Naval Postgraduate School Center for Homeland Defense and Security,
The Homeland Security/Defense Education Consortium,
The Department of Homeland Security Office of Grants and Training,
The Department of Homeland Security Office of the Chief Learning Officer, and the
Critical infrastructure Protection Program, George Mason University
will be hosting the

Homeland Defense and Security Education Summit

George Mason University Feb 27 - 28, 2007

Our organizations, in partnership with academic and a variety of Homeland Security related organizations nationwide, have made great strides in developing and promoting the disciplines of Homeland Defense and Homeland Security. We are gathering in February to:

- Discuss and debate the current state of Homeland Security and Defense Education;
- Receive updates and projections of future efforts from the four event sponsors;
- Provide researchers with an opportunity to present their work on Homeland Defense and Security education;
- Provide academic institutions the opportunity to share, by academic level (associates, bachelors and graduate) highlights of their programs, issues, and challenges;
- Evaluate our responsiveness to the practitioner community's academic requirements;
- Hear the views from top policy authorities on the future direction of Homeland Defense and Security; and
- Discuss research and accreditation issues

Keynote speakers include:

The Honorable Michael Chertoff (Invited), Secretary of Homeland Security
The Honorable Peter Verga, Deputy Assistant Secretary of Defense for Homeland Defense
RADM Jay Cohen USN (Ret.) (Invited), Undersecretary for Science and Technology, DHS

For more information on this invitation-only event, please visit http://www.chds.us/alt.php?special/info&pgm=UAPI_Feb07 or contact Marjan Davey at the Naval Postgraduate School Center for Homeland Defense and Security (medavey@nps.edu or 831-656-2356).

DIB *(Continued from Page 5)*

- Impact on Public Confidence: Effect on public morale and confidence in national economic and political institutions; and

- Impact on Government Capability: Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

Education and Outreach

DoD understands that a successful DIB risk management effort requires effective training, education, and outreach programs. In order to advance these training, education, and outreach opportunities, DoD provides internal DoD programs and supports DIB sector security partners' external initiatives. Target audiences include senior executives and managers, intelligence analysts, assessment teams, and security personnel.

Awareness visits to DIB sites serve as the foundation of the DIB training, education, and outreach activities. The intent of these visits is to educate the audience, particularly facility security and management personnel, as well as local first responders, regarding the national and DoD programs. DoD conducts these visits in cooperation with DIB security partners including the private sector, the National Guard Bureau, DHS, FBI, state and local governments, local first responders and law enforcement officials.

DIB Mission Assurance Assessment Training is provided by the West Virginia National Guard Training Center and is intended for individuals who perform assessments. The training center offers two weeks of training in three levels:

- Overview of the DIB asset prioritization and risk management process with enough detail to conceptually understand what is required to arrive at a protected infrastructure

- Concepts and elements of the assessment process

- Specific assessment techniques

Summary

To fulfill its responsibilities under the NIPP, the OASD(HD&ASA)/DCIP program is a consensus-driven sector security construct that draws on the active, voluntary, and full engagement of all security partners, particularly private sector and other owners and operators. Integration and participation of the private sector will achieve three key areas of value:

- Minimizing service disruption ensures consistent, predictable revenue flow.

- Resiliency and the ability to restore disrupted service provides a competitive advantage.

- Public recognition for preparedness, continuity of service and good corporate citizenship enhance corporate reputations with investors, other customers, and potential employees.

The importance of DIB security partners' contributions to the accomplishment of critical national strategies and programs makes their full and visible engagement an important goal for DoD. Through their full engagement, DIB security partners will obtain improved access to information regarding vulnerabilities, risk assessment, and management best practices. These elements of information will provide a worthy return on investment in the form of continuity in a stressed environment and capability to respond to customer requirements. ❖

Bryan Interview *(Continued from Page 10)*

assessment program and validated it as a requirement. This can help secure funding and bring with it the acknowledged support of senior military officials. We feel it reflects well on the quality of the program and we hope to expand the scope of assessments undertaken around the country.

At present, we have National Guard CIP assessment teams in West Virginia, California, Colorado, New York, Minnesota, and Georgia. There has also been interest expressed by Nevada and Virginia. These teams are trained to DoD approved standards by the West Virginia National Guard at their Joint Interagency Training Center, Camp Dawson, West Virginia. These teams then return to their state, or are deployed to other states, to undertake assessments of CI vulnerabilities. We feel this is an outstanding program and a good example of how DoD, through the National Guard, can use its particular capabilities to contribute to protecting CI in general, and defense CI in particular. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for ***The CIP Report***, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1