Critical Infrastructure Protection

A Primer on the Defense Industrial Base

HDIAC BCO Staff

This is the third in a series of articles for the Homeland Defense and Information Analysis Center (HDIAC) describing the fundamental directives and charters that provide our strategy for Homeland Defense and Security, as well as the Department of Defense's (DoD) role in supporting the National Infrastructure Protection Plan (NIPP). [1] This article describes the DoD plan for protecting our Critical Infrastructure as the Sector–Specific lead for the Defense Industrial Base (DIB).

The Defense Industrial Base

When thinking of the DIB, many people associate the defense industries with the nation's industrial strength that was brought to bear to win World War II. Many remember the war products developed and manufactured by U.S. industries. These industries and technologies created the Jeep, multi-engine propeller driven bombers, carrier fighter aircraft, the Sherman tank, the M-14 and fleets of destroyers, carriers and Liberty ships. As the nation rallied to support the war effort, the "war industry" industrial base ramped up to provide the machines of war on a massive scale. As men were called up to fight the war on two fronts, women enrolled to help the effort as well.

A recent August 11, 2014, Washington Post article titled: "Rosie the Riveter, 70 years later," reminded us of how American women working in industrial factories during World War II contributed to winning the war by out-producing the Axis powers. The American Rosie the Riveter Association estimated that more than 6 million women worked in war industries, helping to produce more than 300,00 airplanes, 100,00 tanks, 44 billion rounds of ammunition and other material. [2]

In the three years following the Battle of Midway, the Japanese built six aircraft carriers. The United States built 17. American industry provided almost two-thirds of all the Allied military equipment produced during the war: 297,000 aircraft, 193,000 artillery pieces, 86,000 tanks and two million army trucks. In four years, American industrial production, already the world's largest, doubled in size. [3] The combined 1940s DIB network of manufacturing plants, far-sighted industrialists and engineers, and our nation's efforts to conserve resources (the United States auto industry produced 3 million cars in 1939 and only 139 more cars until the end of WW II [3]), directly affected the outcome of the war.

Today, the collective DIB has morphed in scope and form from its post WW II production capabilities that allowed massive frontal campaigns and island-hopping strategies. The abilities for large-scale amphibious assaults and massive movements of divisions are not as applicable in the war on terrorism as they were on D-Day or the WWII battlegrounds in the deserts of North Africa or Anzio Beach.

The Cold War changed the requirements once again as more strategic bombers and missile defense and antisubmarine warfare systems were needed. With the end of the Cold War and after the events of September 11, 2001, enemies from non-nation states are engaged in asymmetric warfare against the United States as saboteurs and terrorists. The non-nation-state enemy no longer wears a uniform and rarely attacks with armored divisions, engages in sea battles or has air superiority. Our warfighters today encounter improvised explosive devices delivered by suicide bombers or roadside bombs using remote detonation. The enemy uses snipers, mortars and rocket launchers hidden within local population centers to fight a highly robust technology-based mobile and personal war against the United States. In response, our defense forces need sophisticated Chemical, Biological, Radiological, Nuclear (CBRN) sensors, protective systems for Improvised Explosive Devices (IED), robust communication systems, biometric identification systems and cyber security protection systems.

Production of B-24 Liberators at Ford plant in Detroit, MI. (Understanding Capitalism Part V: Evolution of the American Economy. Price, R.G., March 15, 2013/Released)

Accordingly, the defense industries have had to continue to evolve and innovate with new and better technologies to assist the warfighter. Although the face of the DIB is changing and there are only a handful of shipyards and airplane manufacturers and one major air transport manufacturer, the United States still needs aircraft and ships to move men and equipment to conduct wars on foreign soil. The United States still needs to protect the industries that supply the materials for standing defense forces. Understanding that the way we engage the fight has changed, we also recognize the

warfighter's requirements to fight the war against terrorism have spawned new technologies and new industries to produce advanced weapons that are more precise and surgical. The DIB has grown to include industries that produce Unmanned Aerial Vehicles (UAVs), Global Positioning Satellites (GPS) guided bombs and precision guided weapons, laser weapons, sophisticated missile defenses, satellites, cruise missiles and technologies for cyber warfare. The scope and form of our new industrial base has to be considered when thinking of critical infrastructure and how to protect it.

U.S. Air Force Tech. Sgt. Matthew Green fastens the GPS mechanism inside a RQ-11B Raven B unmanned aerial vehicle at the Eglin range, Fla., Aug. 9. The UAV comes equipped with a GPS in order to track the aircraft when maintaining a visual may not be possible. (U.S. Air Force Photo by Airman Gustavo Castillo/ Released)

So, what does the 21st century DIB look like as we fight the war against terrorism? How do we identify what comprises critical infrastructure protection (CIP), and how does the DoD manage the complexities of a changing and dynamic national industrial base while protecting it from resourceful and ruthless terrorist organizations?

DoD Role in Supporting the National Infrastructure Protection Plan (NIPP)

The Defense Industrial Base Sector Specific Plan [4] provides the DoD's in-depth planning that supports the National Infrastructure Protection Plan. [1] This carefully thought out and detailed plan was modified in 2010 from its original 2007 version. [5] As such, the 2010 plan is described as a dynamic document, taking into account the multiple collaborations between government agencies and the ongoing assessments with regard to infrastructure priorities, capabilities and vulnerabilities.

This plan takes into account 21st century strategies against asymmetric warfare while maintaining a strategic ability to fight globally. Among its many parts, the Plan identifies today's defense industrial base assets and associated segments and sub-segments as described in the following chart:

Industry Segment	Industry Sub-segment	Industry Segment	Industry Sub-segment
Aircraft	Fixed Wing Rotary Wing Unmanned Aerial Systems	**Munitions**	Missile Tactical Missile Strategic Missile Air-Air Missile Air/Surface Missile Defense Missile Surface/Air Missile Surface/ Surface Precision Guided Munitions Ammunition Missile Defense Agency
Ships	Surface Sub-Surface Unmanned U/W Vehicles	**Space**	Launch Vehicles Satellite Missile Defense Agency
Tracked and Wheeled Land Vehicles	Combat Vehicles Tactical Vehicles Unmanned Ground Vehicles	**Mechanical**	Transmissions (Air/ Auto) Propulsion (Diesel/ Rocket/Turbine) Hydraulics Bearings Nuclear Components (including Depleted Uranium)
Electronics	Electronic Warfare Command Control Communications, Computer and Intelligence (C4I)	**Structural**	Castings/Forging Composites Armor (Ceramic/ Plating) Precious Metals
Soldier Systems	Chemical Biological Defense Systems Clothing and Textiles Subsistence/ Medical		

Table of DIB assets and associated segments and sub-segments. (Courtesy of DIB Sector Specific Plan/Released)

The thousands of companies that comprise the DIB assets listed on the previous page provide the research and development, design, production, delivery and maintenance of the military weapons systems, subsystems, components and/or parts to meet U.S. military requirements. The identification of the individual companies that are part of the critical infrastructure protection plan involves a carefully defined screening and vetting process using mission essential tasks defined by the Combatant Commanders.

Naval Research Laboratory has developed and demonstrated technologies for the recovery of CO_2 to hydrocarbons that can be used to produce designer fuel. (U.S. Navy photo by Mass Communication Specialist 3rd Class Gregory Pickett/ Released)

What is Critical Infrastructure for the DoD?

To encompass the broad spectrum of what constitutes today's defense industrial base, the DoD begins by soliciting nominations and screening industries and technologies for impact on national defense missions. The 2010 Defense Industrial Base Sector Specific Plan details responsibilities and requirements for this process as follows: [4]

The Defense Contract Management Agency (DCMA) augments the Combatant Commanders (CCDR) mission analysis by soliciting nominations for DIB critical assets. This additional process ensures a comprehensive examination of possible DIB Critical Infrastructure/ Key Resources (CIKR).

To identify critical asset nominations, DCMA uses the following screening criteria that focus on impact to national defense missions:

- Single source, sole source or defense-unique suppliers
- Suppliers of products that have dual-use qualities
- Suppliers of products that are used in multiple DoD programs
- Suppliers with high requalification cost or long lead requalification timeframes
- Suppliers developing and possessing advanced or emerging technology

The criticality screening process focuses on each industrial facility. As facilities are identified, the crux of providing a protection plan begins to take form. This plan of action provides for real time assessment of vulnerabilities and steps that need to be taken to protect these facilities from sabotage or terrorist attacks.

The DIB Sector Specific Plan describes how DoD, in collaboration with other DIB Sector partners, performs a screening of all candidate DIB critical assets based on the potential consequences of loss or disruption to DoD missions. DoD determines the consequence of loss for DoD-owned assets as part of the overall mission decomposition. If the impact of the loss results in mission failure, the asset is deemed critical regardless of how likely that loss might be. Clearly, potential threats, hazards and exploitable vulnerabilities do not determine the criticality of an asset. Loss of DoD mission capability places the national defense at risk regardless of the reason for the lost capability, hence the dominance of this screening criteria in the DIB Sector risk assessment. This criterion also reflects the importance of the DoD-DIB consumer-supplier relationship in achieving overall mission assurance. It should be noted that the most sensitive information resides in electronic product portfolios on a DoD classified system portal. This repository contains summaries of supporting information on DIB CIKR. The Assistant Secretary of Defense for Homeland Defense & America's Security Affairs (ASD (HD&ASA)) and other DoD decision makers use this information for risk management and continuity of operations purposes. [4]

"The DIB Sector Specific Plan describes how DoD... performs a screening of all candidate DIB critical assets based on the potential consequences of loss or disruption to DoD missions."

How to Assess Vulnerabilities

The DCMA completes DIB CIKR prioritization based on the consequence of loss before conducting asset-specific vulnerability assessments. This ensures that the highest consequence CIKR receives a vulnerability assessment first and facilitates necessary mitigation activities as soon as possible.

The cornerstone of the DIB CIKR vulnerability assessment process is the CIP-Mission Assurance Assessment (MAA). The MAA is conducted by a State National Guard team. Based on the prioritization of CIKR, DCMA will coordinate a schedule with CIKR owners and operators for CIP-MAAs that are conducted by the National Guard. A CIP-MAA considers an "on-the-ground" refinement of the impact (consequence of loss) and evaluates the exploitability of a wide range of vulnerabilities and risk vectors. The CIP-MAA also evaluates plausible threats/hazards from natural disaster, technological failure, human error, criminal activity or terrorist attack. This approach ensures consideration of relevant factors for each DIB asset as well as the relative prioritization of risks to DoD missions. Through FY 2009, the SSA has completed comprehensive vulnerability assessments at 52 critical DIB asset sites. Aggregate analysis is currently underway to identify trends in risk profiles, dependencies, lessons learned and best practices across the sector. The SSA plans to refine this analysis and incorporate future assessment results to share findings with industry and government stakeholders going forward. [4]

The DoD 2010 DIB Sector Specific Plan (SSB) Updates

Since publication of the 2007 DIB SSP, the following major steps have been taken to identify and update the inventory of DIB CIKR: [4]

- DCMA and DIB members identified potential suppliers meeting screening criteria.
- The Military Departments, DCMA and other Defense Agencies have validated and updated the list of potential DIB CIKR.
- DCMA has coordinated the DIB Critical Asset List (CAL) with Military Department acquisition executives and Defense Agency directors.
- DCMA has submitted the DIB CAL to Deputy Undersecretary of Defense (DUSD) for Industrial Policy and then to Undersecretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L) for approval.
- The ASD(HD&ASA) have notified DIB CIKR owners/operators of their criticality designation.
- The ASD(HD&ASA) has submitted the DIB CAL and Important Capabilities List (ICL) to the Department of Homeland Security (DHS).

The DoD continues to work with DHS and other Sector Specific Agencies (SSAs) to identify overlaps and gaps in responsibility for DIB assets. The DIB SSA also interacts with its partners under a flexible approach based on relevant circumstances. DoD maintains basic data on all DIB partners. This data provides a general characterization of potential critical assets, systems and networks. There are no regulatory requirements to provide infrastructure data among DIB partners. DIB asset owners provide data on a voluntary basis with assurances that DoD employs appropriate measures and procedures to protect business-sensitive and proprietary information.

In addition to the activities described above, DCMA leverages its global contract management enterprise to acquire, validate, maintain and protect fundamental industrial data and specific DIB asset data. Tools, networks and associated policy documentation are currently under development and implementation to facilitate these data collection and retention processes. [4]

Air Force Staff Sgt. Jennifer Hurley, 673d Dental Squadron dental technician, applies a moulaged arm wound to Airman 1st Class Corey Williams, 3rd Operations Support Squadron air traffic controller, in preparation for Mission Assurance Exercise 14-3 on Joint Base Elmendorf-Richardson, Alaska, March 27, 2014. JBER's MAE 14-3 aims to test the base's ability to operate during a major natural disaster. (U.S. Air Force photo by Senior Airman Omari Bernard/Released)

Example of Risk-Mitigation and Enhanced Outer-Perimeter Security. (Courtesy of William F. Booth, CPP/Released)

Metrics for Success

The DIB 2010 Sector-Specific Plan also provides a detailed plan for measuring the effectiveness of DoD's protection of the defense industry's critical infrastructure. The 2010 plan is the first reporting of these metrics and is designed to collect data that reflects the dynamic nature of the recommended risk mitigation efforts commensurate with updated risk assessments. The metrics measure the effectiveness of the CIP MAAs recommendations conducted by the DoD for many of the critical industry segments. The detailed Measurement Effectiveness plan described in Chapter 6 of the 2010 Defense Industrial Base Sector-Specific Plan states: "The performance and outcome metrics enable DoD and the DIB to establish accountability, document actual performance, facilitate the diagnosis of problems, promote effective management, make decisions and provide feedback to senior decision makers in the DIB partnership." The Measurement Effectiveness Plan allows for annual reviews, updates and monitoring of the metrics program.

Other Considerations

In a recent memorandum from the Office of Management and Budget and Office of Science and Technology, multi-agency research and development priorities were proscribed for the 2016 budget, which stated, in part, that the Administration is "committed to revitalizing America's manufacturing sector, which will require innovation in the products that are manufactured and the manufacturing systems themselves. Agencies should give priority to those programs that advance the state of the art in manufacturing, with particular emphasis on government-industry-university partnerships and enabling technologies for industries of the future (such as nanotechnology, robotics, materials development and cyber-physical systems) that benefit multiple sectors, as described in the National Strategic Plan for Advanced Manufacturing." [6]

In view of the above, and the recognition by both the Secretary of Defense and the Under Secretary of Defense for Acquisition, Technology and Logistics that the proliferation and development of advanced military technologies make it difficult for continued military dominance by U.S. forces, we can understand why the landscape of our defense industry needs to change. The recent August 21, 2014, *War on the Rocks* commentary by Harrison and others, titled: "A New Defense Innovation Base," describes the change as follows:

"...the explosion of global public and private R&D investment has led to the proliferation of increasingly sophisticated component, design, prototyping and manufacturing technologies, enabling a new generation of innovators and threats that learn in rapid, iterative cycles. In short, the steady state threat and technology environments around which the legacy defense acquisition system and the defense industrial base came into being in the Cold War have been replaced by an uncertain, rapidly evolving world subject to disruptions that cannot be predicted or planned for with a high level of certainty. It is within this innovation environment that DoD must now compete." [7]

Accordingly, our ability to protect our evolving critical infrastructure through processes contained within the National Infrastructure Protection Sector Specific Plans remains paramount to the protection of our DIB.

How HDIAC Contributes

The Homeland Defense Information Analysis Center (HDIAC), one of three Information Analysis Centers managed by the DoD IACs enterprise administered under the Defense Technical Information Center (DTIC), is tasked to collect, analyze, synthesize, produce and disseminate worldwide scientific and technical information (STI) and drive innovation and technology developments by anticipating and responding to the information needs of the defense and broader community, while enhancing collaboration through integrated STI development and dissemination. The IACs continue to use this ability to enhance their Technology Domain Awareness (TDA). TDA is the effective understanding of the technology landscape as it relates to current and future defense capability needs. "It is predicated on timely, relevant and accurate knowledge of the 'technology commons'" - those areas where global leadership in technology development and application are increasingly spread across multiple nations and non-state interests. As defense-relevant innovations increasingly occur in commercial markets, the IACs' TDA efforts seek to expand awareness and application of commercial and non-government

investments to enable better, cheaper and faster Defense capability development." [7]

Although still in its formative stages, HDIAC hopes that the TDA initiatives will promote the following:
TDA initiatives will provide "…faster, more cost-effective defense capability development capitalizing on commercial market efficiencies, networked knowledge and lessons learned from past engagements. TDA will provide a defense-wide platform for identifying, synthesizing and amplifying technology-based innovations and lessons learned in order to enhance scalability, adoption and impact while improving defense stakeholder awareness of "outside innovations"– technologies derived from, or underwritten by, the commercial (non -defense) R&D marketplace." [8]

Furthermore:
"… the TDA seeks to build an extended defense-focused innovation base that (1) informs the existing defense acquisition enterprise by broadly aligning innovative commercial and consumer-facing products with defense applications; (2) complements the defense industrial base by creating a flexible, scalable industry platform, where businesses and institutions primarily focused on non-defense markets can easily "opt-in" to support the rapid, cost-effective development of new defense capabilities." [8]

As noted in other guiding documents, the preservation of knowledge and development of a defense-focused innovation base are critical for solving current problems and meeting future challenges. The actions taken to identify and protect the Nation's infrastructure from an ever increasing threat of a terrorist action using Weapons of Mass Destruction or a "lone wolf" attempt to cripple one sector of our national infrastructure need to be communicated and made readily available to our government interagency partners to maximize our effectiveness. The IACs serve to facilitate that communication.

References:

[1] National Infrastructure Protection Plan (NIPP), Partnering to enhance protection and resiliency, June 2009.
[2] The Washington Post, August 11, 2014, Julie Zauzmer, Rosie the Riveter, 70 years later.
[3] The War At Home, War Production, PBS, September 2007. http://www.pbs.org/thewar/at_home_war_production.htm.
[4] Department of Defense, Defense Industrial Base Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan, May 2010.
[5] Department of Defense, Sector Specific Plan for the Defense Industrial Base in Support of the National Infrastructure Protection Plan, May 2007.
[6] Deese Brian C., Director of Management and Budget, Executive Office of the President of the United States and Holdren, John P., Office of Science and Technology Policy, Executive Office of the President of the United States, M-14-11, July 18, 2014: MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES. Subject: *Science and Technology Priorities for the FY 2016 Budget.*
[7] http://iac.dtic.mil/tda.html
[8] Harrison, Adam Jay; Rachami, Jawad; Zember, Christopher, "A New Defense Innovation Base," *War on the Rocks*, August 21, 2014, in Commentary. http://warontherocks.com/2014/08/a-new-defense-innovation-base/.