



THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 9 NUMBER 11
AND HOMELAND SECURITY

MAY 2011
DEFENSE INDUSTRIAL
BASE SECTOR

Sector Overview	2
DIB Challenges	7
NDIA	9
Legal Insights	11
SARMA and GITA	15
WEIS	16
WOICI	17

EDITORIAL STAFF

EDITORS

Devon Hardy
Olivia Pacheco

STAFF WRITERS

M. Hasan Aijaz
Shahin Saloom

JMU COORDINATORS

Ken Newbold
John Noftsinger

PUBLISHER

Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

Click [here](#) to subscribe. Visit us online
for this and other issues at
<http://cip.gmu.edu>

This month's issue of *The CIP Report* highlights the Defense Industrial Base (DIB) Sector. This Sector is responsible for providing the products and services essential to mobilizing and sustaining this Nation's military operations.



School of Law

CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

First, representatives from the Defense Industrial Base Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) provide an overview of the DIB Sector. Next, a Senior Policy Analyst for National Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation discusses the current status of the DIB Sector. The National Defense Industrial Association (NDIA), in a previously published policy/issue paper, then expounds upon four main themes that need to be addressed to sustain a successful manufacturing policy within the DIB Sector.

This month's *Legal Insights* describes and evaluates the recent decision of the United States Air Force (USAF) to award the Boeing Company the task of developing new air refueling tankers.

We also include a "Save the Date" for the 5th Annual Security Analysis and Risk Management Association (SARMA) Conference. The theme of the conference is "Security Risk 10 Years After 9/11: How Far Have We Come and What Lies Ahead?" Finally, there is an announcement for the 20th Annual GIS for Oil and Gas Pipeline Conference as well as a reminder about the 10th Workshop on Economics of Information Security (WEIS) and the Workshop on Cybersecurity Incentives (WoCI).

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

The Defense Industrial Base Sector

by Charles Kosak, Acting Deputy Assistant Secretary of Defense for Homeland Defense Strategy, Force Planning and Mission Assurance, Chair — Defense Industrial Base Government Coordinating Council, U.S. Department of Defense, and
Major General Barry Bates, USA (ret), Chair — Defense Industrial Base Sector Coordinating Council, National Defense Industrial Association

Defense Industrial Base Sector Overview

Critical infrastructure and key resources (CIKR) are essential to the Nation's security, economic vitality, and way of life. Accordingly, national policy objectives require Federal departments and agencies to identify and prioritize CIKR, to enhance CIKR protection against attacks, and to strengthen resilience for a range of manmade or national hazards. Recognizing that each critical infrastructure sector possesses its own unique characteristics, operating models, and risk landscapes, national policy also designates a Sector-Specific Agency (SSA) to oversee each of the 18 national infrastructure sectors. The Department of Defense (DoD) is the SSA for the Defense Industrial Base (DIB) Sector and leads a collaborative, coordinated effort to identify, assess, and improve risk management of critical infrastructure within DIB. The DIB Sector's vision is to collaboratively eliminate or mitigate unacceptable levels of risk to physical, human, and cyber assets, thus ensuring that DoD continues to fulfill its mission; and that DIB activities continue to effectively support national security objectives, public health and safety, and public

confidence.

DIB is defined as the worldwide industrial network with capabilities to perform research and development, and to produce, deliver, and maintain military weapon systems, subsystems, or components. It is composed of hundreds of thousands of worldwide government and private sector sites, with the majority of them being privately owned. DIB companies can range from small proprietors to Fortune 500 corporations employing tens of thousands of people. Contrary to common belief, DIB does not include commercial infrastructure, such as power or other utilities. These commercial infrastructures are addressed by other SSAs. Defense-related products and services provided by DIB equip, inform, mobilize, deploy, and sustain forces conducting global military and humanitarian operations. DIB companies are subdivided into segments and sub-segments that produce weapon system platforms, components, and expendables. This categorization is used by DoD to classify the contributions of particular DIB assets, as well as to analyze the criticality of the assets within the Sector. Figure 1 (on page 3) outlines

those segments.

Key Collaborative Forums

Effectively executing SSA responsibilities requires significant collaboration between the various DoD organizations that have DIB responsibilities, industry partners, and other Federal departments and agencies. Many DoD organizations have responsibilities that support national CIKR protection objectives. Implementing national SSA responsibilities requires significant coordination across DoD components. Policy and DoD roles and responsibilities for critical infrastructure are included in DoD Directive 3020.40, available at: <http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf>.

Voluntary partnership is a central tenet of national efforts to build more secure and resilient U.S. infrastructure and to DoD's efforts to identify, assess, and improve DIB resilience. To implement its SSA responsibilities, DoD uses several key forums:

- **DIB Government Coordinating Council (GCC):**
We partner with 6 Federal Departments that have equities

(Continued on Page 3)

Sector Overview (Cont. from 2)

impacting DIB. These include the Departments of State, Treasury, Justice, Commerce, Homeland Security, and most recently, the Department of Energy.

- DIB Sector Coordinating Council (SCC):** The DIB SCC is chartered as the framework enabling DIB private sector owners and operators to engage DoD, the Department of Homeland Security (DHS) and SSA on matters related to CIKR resilience. Six defense industry associations and 22 companies make up the DIB SCC.
- DIB Joint Coordinating Council Meetings:** The GCC, SCC, and select subject matter experts meet quarterly to discuss and resolve joint efforts related to DIB. These meetings are conducted under the DHS Critical Infrastructure Public Advisory Council (CIPAC) framework to allow for a free exchange of information between industry and government on critical issues.
- DIB Critical Infrastructure Protection Conference (DIB CIP):** An annual conference co-sponsored by the National Defense Industrial Association (NDIA) and DoD that addresses security and resilience of the Sector. The 2011 theme is “DIB CIP 2020: Setting the Vision & Strategy for the Next Decade.” Senior level speakers and panelists will address core topics such as: Managing Risks, DIB Cyber Mission Assurance, Infrastructure Dependencies, Information Sharing, Preparedness Resiliency and Response, Recovery and Reconstitution. For more information on the postponed 2011

Figure 1: DIB Segments and Sub-segments

AIRCRAFT	Fixed Wing	C4I	Strategic C4	
	Helicopter		Tactical C4	
	Unmanned Aerial System		Night Vision/Infrared	
SHIPBUILDING	Surface Ship		Electronic Warfare	
	Sub Surface Ships		Ground Stations/Data Links	
	Unmanned Underwater System		Navigation Systems	
AMMUNITION	Ammunition (Large Caliber)		GROUND VEHICLES	Signal Warfare
	Ammunition (Medium caliber)			Tracked Vehicles
	Ammunition (Small Caliber)			Wheeled Vehicles
	Artillery		SOLDIER SYSTEMS	Troop Support
	Bombs/Bomb Accessories	Chem Bio Defense (various)		
	Dispenser Munitions	Precision Guided Munitions		
	Flares	Strategic		
	ARMAMENTS	Grenades	MISSILE	Tactical
		Mines		Satellite
		Mortars	SPACE	Launch Vehicle
Rockets & Warheads		Ground Stations		
Cannon				
Man Portable				
Mounted				

DIB CIP Conference, please visit the NDIA website at: <http://www.ndia.org/meetings/1030/Pages/default.aspx>.

- Enduring Security Framework (ESF):** The ESF is a public-private forum of senior leaders in both industry and government focused on information and communication technology matters, including cybersecurity and other information assurance threats. The Executive Council includes the Deputy Secretary of Defense, the Deputy Secretary of Homeland Security, the Director of National Intelligence, and Chief Executive Officer (CEO) level industry executives. The operations working group focuses on DIB issues and brings industry and government together to mitigate emerging and current cyber-based threats to DIB and associated technology bases. DIB GCC and SCC leaders participate in this forum.

DIB Roles and Responsibilities

Many DoD organizations have responsibilities that support national CIKR protection objectives. Implementing national SSA responsibilities requires significant coordination across DoD components. Table 1 (see page 5) outlines some of the key DoD players and their primary DIB roles.

Joint Objectives

Under the leadership of the combined Government and Sector Coordinating Councils, the DIB Sector developed a Joint Business Plan (JBP) to focus annual activity on a set of shared objectives. These objectives are based on the goals of the DIB Sector Specific Plan and on current trends or threats that impact DIB. This joint plan identifies concrete and action-oriented

(Continued on Page 4)

Sector Overview (Cont. from 3)

objectives with assigned timelines and responsible leads. The JBP reenergized DoD and private sector engagement within the national CIKR protection framework and set about making concrete progress for resilience functions throughout the Sector. The 2010 JBP has 22 objectives organized into five focus areas: Criticality, Threat Comprehension, Dependency Analysis, Assessments, and Information Sharing.

Criticality: DoD oversees the annual process that determines the criticality of private sector DIB assets vital to DoD missions. Annually, DoD civilian and service components nominate assets that meet these criteria to identify important or critical capabilities necessary to maintain DoD missions. This year, for the first time, our industry partners will also be engaged in this critical asset identification and prioritization process. DoD recognized that the DIB SCC has valuable knowledge of industry capabilities, supply chains, dependencies, and vulnerabilities that could help shape the annual critical asset list.

Threat Comprehension: DoD is working to address several key threats identified as DIB priorities, including cyber threats, insider threats, and front companies. DIA's Joint Intelligence Task Force — Counter Terrorism (JITF-CT) now provides periodic classified threat briefings on topics of interest to DIB SCC partners. The true success of these roundtable discussions is the resulting relationship and trust building between the intelligence community

and the private sector.

Dependency Analysis: Understanding DIB dependency on other critical infrastructure sectors is vital to DoD's ability to engage in interagency process and to advocate for risk management of those dependencies. The Department is analyzing existing assessment data to identify DIB energy dependency trends to provide DIB partners a baseline for analyzing their facilities. Additionally, DoD will undertake two regional energy dependency assessments by the end of the fiscal year and provide a dependency methodology for use by DIB partners.

Assessments: DIB critical assets are currently assessed by various DoD components and other Federal agencies. The companies themselves also identify risk and validate security, functionality, and resilience. DoD is examining ways to streamline DIB assessments and share assessment results more widely among organizations with DIB responsibilities. One key initiative is an agreement between DHS and DoD that will begin more focused joint assessments of DIB facilities and allow the two organizations to share the data gathered from past and future assessments.

The SCC plans to implement physical security, cybersecurity, and resilience self-assessment tools that will produce a relative score for each facility and allow DoD and DHS to focus assessment efforts. A concise DIB Sector physical security self-assessment tool has been designed for small and medium size

companies and is available to DIB companies on the Homeland Security Information Network (HSIN) DIB portal.

Information Sharing: A significant issue of concern is increasing information sharing capabilities, mechanisms, and practices with DIB. Both industry and government partners identified their information sharing requirements as a baseline for future initiatives.

A first step to improve information sharing was recently completed by DHS and the DIB SCC by developing and deploying a private sector portal on the HSIN. This tool enables CIKR owners and operators to access threats, warnings, and risk information. It also allows them to participate in discussions, awareness webinars, and other types of collaboration. To request access to the HSIN-DIB portal, private sector companies should submit their name, title/position, company, or organization and work email address to cikriseaccess@dhs.gov.

DoD has identified existing information sharing portals and is pursuing the national goal of a federated set of authoritative portals that allow industry stakeholders to visit one site for all of their information sharing needs. DoD is also pursuing a system to host a robust two-way information sharing mechanism at the classified level. DoD recently implemented an emergency notification system that can reach DIB SCC partners, and will be expanded over time to the

(Continued on Page 5)

Sector Overview (Cont. from 4)

Table 1: DoD Component DIB Roles and Responsibilities	
DoD Component	Responsibilities
Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))	AT&L sets industrial policy and manages the multi-billion dollar procurement process, including the customer- vendor relationship with industry. AT&L is responsible annually for development and documentation of privately held DIB assets that are critical to maintaining DoD missions.
Under Secretary of Defense (Intelligence) (USD(I))	USDI frames policy and oversees intelligence, counterintelligence, and security support, as appropriate, to the national DIB Sector. This includes establishing national DIB Sector intelligence requirements that are reflected in Combatant Command, the Services, DoD, and national collection plans. USDI also manages industrial security policy, which establishes the requirements for cleared DIB members to safeguard classified information in their possession while performing work on contracts, programs, bids, or research and development efforts.
Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs (ASD(HD&ASA))	The Secretary of Defense delegated SSA responsibilities for the DIB to Under Secretary of Defense for Policy. HD&ASA under the USD(P) develops DoD policy, productive partnerships, and strategies to enhance the security and resilience of the DIB in coordination with National CIKR policy objectives. HD&ASA leads key DIB collaboration forums and is responsible for overall critical infrastructure policy development within DoD.
Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))	ASD (NII) implements the Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) pilot, which was established in 2007 by the Deputy Secretary of Defense with the support of an initial small group of DIB Chief Executive Officers (CEOs). The mission of this program is to improve protection of critical DoD unclassified program and technology information residing on, or transiting, DIB unclassified systems and networks. This collaborative information assurance program involves cyber threat information sharing, incident reporting and remediation, and intrusion assessments of compromised data. Based on lessons learned and with procedures in place, the DIB CS/IA program is transitioning from a pilot status to a full program that will allow participation by all qualified defense contractors. The qualifications will be in an Interim Final Rule published in the Federal Register, date to be determined (expected Summer 2011). Planning is also underway for a follow-on pilot with non-cleared defense contractors.

(Continued on Page 6)

Sector Overview (Cont. from 5)

Table 1: DoD Component DIB Roles and Responsibilities	
DoD Component	Responsibilities
Deputy Assistant Secretary of Defense for Cyber Policy	Develops DoD strategy and policy for operations in cyberspace. Responsible for the oversight of DoD cybersecurity activities in support of the DIB and the other agencies of the U.S. Government.
Defense Contract Management Agency (DCMA)	DCMA’s Industrial Analysis Center (IAC) manages the relationship with the DIB through their Contract Management Offices. The Homeland Defense division performs mission-focused vulnerability assessments on DIB assets. IAC also provides trend analysis related to DIB resiliency, analyzes mission impact during DIB incidents, manages the annual criticality identification process, and identifies DIB resiliency initiatives.
Defense Security Service (DSS)	DSS is a member of the DIB GCC and is responsible for securing the Nation’s technological base and overseeing the protection of U.S. and foreign classified information in the hands of industry. DSS also clears industrial facilities, personnel, and associated information systems, which includes security inspections; collects, analyzes and provides threat information to industry and government partners; provides advice to industry; delivers security education and training, and provides information technology services that support the industrial security mission of DoD and its partner agencies.
Military Services	Each of the Services maintains acquisition and security relationships with DIB members. The Services conduct vulnerability assessments and are a key voice in determining critical DIB assets. They manage the risk of loss or degradation of critical infrastructure and incorporate defense critical infrastructure into education, outreach and training programs, including the testing and exercising of mitigation and response plans.
The National Guard	The National Guard supports the organization and training of DIB vulnerability assessment teams in collaboration with DCMA.

Table 1: DoD Component DIB Roles and Responsibilities

(Continued on Page 18)

U.S. Defense Industrial Base at a Turning Point

by Mackenzie Eaglen*
Heritage Foundation

Last year, the Obama Administration, Secretary of Defense, and Congress began reshaping the U.S. military by changing the direction of defense investments and canceling programs with a total lifetime value of over \$300 billion (if seen through completion). The list of defense cuts include a combat search and rescue helicopter; the F-22 fifth generation fighter; the Army's future combat systems (primarily a ground vehicle program); the multiple-kill vehicle for missile defense; a bomber for the Air Force; the VH-71 presidential helicopter; a transformational satellite program; and the second airborne laser aircraft. In addition, the Administration decided to extend the construction of an aircraft carrier by an extra year from four to five, reduce the number of ground-based midcourse defense interceptors from 44 to 30, and indefinitely delay the Navy's next generation cruiser.

Furthermore, the current Fiscal Year 2011 defense budget is not being spared the axe. Some of the planned reductions include ending production of the country's only wide-bodied cargo aircraft, the C-17; terminating the EPX

intelligence aircraft; permanently canceling the Navy's cruiser; ending another satellite program; and killing the expeditionary fighting vehicle program for the Marine Corps. The Army's surface-to-air missile program and its non-line-of-sight cannon are also slated to end. The Marine Corps now has its version of the Joint Strike Fighter on probation.

Some of these cancellations, including the presidential helicopter, next generation bomber, the Army's combat fighting vehicle, and the Marine Corps' amphibious assault vehicle will be resurrected in future defense budgets because the need for them has not gone away. These program cancellations or deferrals should be taken in context. Of the roughly \$400 billion the DoD spends on goods and services per year, over half of that amount goes to service contracts, not equipment. The cuts to major manufacturing production lines and the defense industrial base are significant, since one in ten American manufacturing jobs is in the defense industry.¹

Additionally, the defense spending outlook for the coming years shows

defense budgets declining in real terms. As part of Washington's efforts to "reduce enormous budget deficits, other defense accounts (from the base or 'peacetime' budget) might decline by 5 to 10 percent given the most current ideas and plausible projections now available. Taken together, these two effects could reduce funds directed to American defense companies by well over \$100 billion a year, or at least one third."²

Aerospace, Shipbuilding, and Defense Workforce Shrinking

America's defense manufacturing industrial base continues to shrink because of defense investment decisions over the past two decades and is accelerating due to budget decisions approved the past two years. This is worrisome on a policy level but also on a practical level. Many of these significant changes are being made in the absence of any careful evaluation of America's global mission. This could lead to hollow security commitments around the world or, worse, a modern-day hollow force.

(Continued on Page 8)

¹ Charley Keyes, "Defense Industry Braces for Shutdown," CNN, April 7, 2011 at http://money.cnn.com/2011/04/07/news/economy/defense_contractors_shutdown/index.htm.

² Michael O'Hanlon, "The National Security Industrial Base: A Crucial Asset of the United States, Whose Future May be in Jeopardy," The Brookings Institution, February 2011, p. 4, at http://www.brookings.edu/-/media/Files/rc/papers/2011/02_defense_ohanlon/02_defense_ohanlon.pdf.

DIB Challenges *(Cont. from 7)*

The U.S. military relies heavily upon the highly-skilled workforce to build the most cutting-edge systems that have given the United States its technical overmatch against our enemies for decades. The workforce hourly wage in aerospace and defense leads all industry sectors, including technology and government. The combined effects of a shrinking workforce and the graying of this industry are problems without clear solutions identified or agreed upon by policymakers.

Over the last decade, the aerospace and defense workforce fell from over one million to 600,000 people. In the past two years, since the latest round of modernization cuts began, over 40,000 direct aerospace and defense jobs have been lost. In reality, this number is much higher (by a factor of three) because of the effect on the second and the third tier jobs that support production line workers. Furthermore, the challenge posed by the aging of the defense industrial base is now growing beyond designers and engineers to include highly-skilled assembly line workers.

These trends are even more troubling when considering that the aerospace industry is a net export leader for the United States. Indeed, several major defense lines are sustained only through foreign military sales. The number of such lines is growing as the number of “new start” U.S. major programs decline. For the first time in the history of aviation (100 years), the United States has no manned commercial or military aircraft

under design. Policymakers face the challenge of how to sustain the military’s technological edge as the number of defense programs decline qualitatively and quantitatively. Expertise in this industry builds slowly. Once highly-skilled workers exit the Federal workforce, they are difficult to recruit back and more expensive to retrain.

The size and talent of the defense industrial base will continue to shrink. This will reduce contractor competition that helps save taxpayer money and spurs additional innovation in unique military technologies. A loss of innovation and an increase in uncertainty facing the companies, vendors, and suppliers that comprise this critical workforce will put this national asset at risk.

How to Reverse the Decline

Continuous replacement of military platforms is vital to ensuring a superior fighting force. In less than ten years, the number of major defense contractors has fallen from fifty to six. Ten years ago, America boasted six major aircraft producers, while today we have only two. Securing America’s military dominance for the decades ahead will require:

- An industrial base that can retain a highly-skilled workforce with critical skill sets, and
- Sustained investment in platforms that offer future commanders and civilian leaders a vital set of core military capabilities and equipment to respond to any threat.

In order to properly guide future defense investments, an industrial policy must include substantial input from defense acquisition leaders, program managers, systems engineers, compliance managers, auditors, and other experts. Defense leaders should also constantly assess the health of the defense supply chain. The next national defense strategy should discuss in detail the ability of the industrial base to respond rapidly to the changes in strategic environment.

Specialized design, engineering, and manufacturing skills are the critical workforce ingredients in sustaining an industrial base capable of building next-generation systems. Already at a turning point, the potential closure of major defense manufacturing lines in the next five years with no additional scheduled production could shrink this national asset even further. While the manufacturing workforce alone should not dictate acquisition decisions, the potential “brain drain” must be considered when Congress determines whether or not to permanently shut down major production lines — particularly shipbuilding and aerospace.

Congress should broadly support increase in foreign military sales between the United States and its allies and partner nations. America’s defense industrial base serves an important role in building the military capacity of foreign allies and enhancing their interoperability with the U.S. military. These efforts

(Continued on Page 20)

National Defense Industrial Association Position Paper on the Defense Industrial Base

by National Defense Industrial Association (NDIA)

This article is the condensed version of a previously published position/issue paper written for the current edition of NDIA's [Top Issues for 2011](#). For full access to this paper, please click [here](#).

America's military strength remains vital to preserving the Nation's interests and sustaining international stability. While much of this strength is derived from the professionalism and skills of America's armed forces, the technologically superior military platforms developed and produced by the U.S. defense industrial base have been vital to ensuring a superior fighting force. In both peace and war, America's defense manufacturing industrial base has allowed the United States to meet the full spectrum of missions the military has been called upon to fulfill. Securing America's military dominance for the decades ahead will require an industrial base that can retain a highly-skilled workforce with critical skill sets and sustained investment in platforms to respond to any potential threat.

U.S. national security depends heavily upon our domestic manufacturing capabilities and DoD relies upon the U.S. defense industrial base for leap-ahead, innovative technologies with which to equip our warfighters. It is critical to understand that in the

defense sector, if the government does not fund a particular system, industry will abandon the effort, including the underlying industrial capabilities. Work force and resources will move on to other funded programs. The segment that is not funded will eventually wither and industry will lose that capability. Once lost, these domestic capabilities take substantially more time and funding to regain. The U.S. industrial base is in crisis and needs attention, and based upon several key studies, the U.S. defense industrial base is facing a similar and parallel crisis. Moreover, the current government procurement policies will not produce the competitive, responsive, efficient, and innovative industrial base that is required to face these challenges.

There are four main themes that need to be addressed to sustain a successful manufacturing policy: leadership and cultural perceptions; research and development (R&D) in manufacturing; strategic manufacturing capabilities for national security; and workforce and infrastructure.

Leadership and the Cultural Perceptions

The health of the defense industrial base has to be elevated to a higher level in the scope of U.S. policy

considerations. This requires active and senior leadership, both within the Administration and DoD. The U.S. agriculture sector represents one percent of our Gross Domestic Product (GDP), employs 1 percent of the workforce, and is represented by a cabinet Secretary. The manufacturing sector is ten times larger and is represented by an Assistant Secretary for Manufacturing and Services within the International Trade Administration of the Department of Commerce. Manufacturing and the industrial base are important enough for representation by at least a Deputy Secretary, which would also raise the level of coordination between government agencies.

In turn, defense manufacturing issues need more senior leadership within DoD to unite policy, strategy, investment, and implementation. Currently, DoD has a Director for Industrial Policy, with responsibility for stimulating competition and sustaining industrial capabilities within the defense industrial base. This office monitors the industrial base and uses established authorities to promote competition or defense priorities over commercial production such as the Defense Production Act.¹ However, DoD requires senior leadership for

(Continued on Page 10)

¹ Public Law 81-774 enacted on September 8, 1950, in response to the start of the Korean War.

NDIA (Cont. from 9)

manufacturing which has the authority to define strategy and set policy, but also implement R&D alignment, infrastructure revitalization, and workforce investment across all of DoD. There is also a problem in the United States with the perception of manufacturing. In a recent survey by the Manufacturing Institute and Deloitte, 81 percent of respondents believe that America's manufacturing base is either important or very important to their standard of living and to economic prosperity, and 77 percent think the United States needs a more strategic approach to the development of its manufacturing base. However, only 30 percent of respondents would encourage their children to pursue a manufacturing career. The perception is that manufacturing is something akin to an iron foundry in the year 1900, but the reality is a manufacturing workforce is as likely to use a keyboard as a wrench, and operates in a clean, safe environment. The government needs to change this outdated perception in order to get the high-caliber workforce needed for high-tech manufacturing, particularly in the defense sector where the workforce is aging.

Research and Development

Manufacturing research and development is literally the core of an innovation machine that this Nation's economic engine is founded upon. Specifically, 70 percent of industrial R&D is performed by manufacturing-based companies, and the bulk of that

R&D is applicable to manufacturing processes and procedures. This R&D results in the application of new technologies, new materials, and overall increased productivity within the manufacturing processes. All of these advances can make U.S. manufacturing more competitive within the global market, but only if the results of the R&D stay in the United States and add to the GDP for a significant period.

The Federal government has a role in the determination of R&D priorities, development of R&D clusters, investments for national security, and leveraging/incentivizing private industry investment. A crucial need at the macro level is the planning and management of a collaborative and highly connected research enterprise which spans large and small businesses, academia, and government research laboratories. Recent studies of best in class foreign R&D strategies have concluded that developing regional "clusters" of specialized R&D partners provide the most effective model for government, academic, and industry innovation, and increase the probability of transition to domestic manufacturing capabilities. These clusters also offer the highest leveraging potential for government investment and have proven to drive associated capital investment in regional facilities and infrastructure.

Strategic Capabilities for National Security

One of the most critical balancing

acts within the industrial policy domain is between open market competition and the creation or subsidizing of a domestic industrial capability. Industrial capabilities in manufacturing processes, raw materials, components, and technologies are disappearing from the United States every day in the form of off-shoring, business failures, supplier mergers, material shortages, global environmental restrictions, and lack of demand. In some cases, disappearing domestic capabilities can be replaced with overseas suppliers, but this is not possible for defense-essential capabilities, where access to domestic sources is a national security requirement. The current DoD industrial policy is to rely on market forces (competition) to create, shape, and sustain the industrial, manufacturing, and technological capabilities necessary to provide our fighting forces with systems that can engage and win full-spectrum warfare. However, when absolutely necessary, DoD will intervene to create and/or sustain competition, innovation, and essential industrial capabilities. If intervention is warranted, DoD can use mechanisms such as direct investment in supplier infrastructure, leveraging R&D investments, procurement assistance, purchase commitments, or collaboration with other Federal agencies to drive growth in domestic vendor demand.

Another critical issue is the need for steady, long-term access to affordable raw materials.

(Continued on Page 19)