NDIA
National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

TOP ISSUES 2013

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION

ISSUE 1:
Maintain a Responsive Defense Industrial Base During Budget and Infrastructure Reductions

ISSUE 2:
Improve Efforts to Sustain Cybersecurity of Critical Infrastructure

ISSUE 3:
Address Energy Security Challenges

ISSUE 4:
Evolve IT Acquisition in a Budget Constrained Environment

ISSUE 5:
Address Improvements Needed to the Procurement Process

ISSUE 6:
Ensure Efficiencies and Education in Department of Defense and Industry Processes

ISSUE 7:
Reform Export Controls to Ensure Competitiveness of US Industrial Base

ISSUE 8:
Improve Small Business Awareness, Opportunity and Utilization in Government Contracts

NDIA
National Defense Industrial Association

National Defense Industrial Association

2111 Wilson Boulevard, Suite 400
Arlington, Virginia 22201-3061
Tel: (703) 522-1820 • Fax: (703) 522-1885
Web page: http://www.ndia.org

The Voice of the Industrial Base

IMPROVING GOVERNMENT-INDUSTRY DIALOGUE IN THE FACE OF SIGNIFICANT FISCAL CHALLENGES

An open letter from the President and CEO of the National Defense Industrial Association

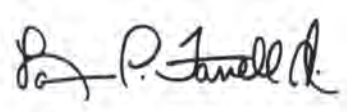
As the nation faces a draw down in overseas operations and continued austerity measures at home and abroad, the defense industrial base realizes that there will be a shift in the way the department buys goods and services. Since its inception in 1919, the National Defense Industrial Association has served as a 'communications bridge' between Department of Defense (DoD) agencies, offices and Military Components, and defense industry companies facilitating an important professional dialogue on the best and most efficient ways to support our troops with best-in-the-world products, services and training. NDIA's many public conferences, symposia, exhibitions, workshops and seminars have been the principal vehicles for this collaborative exchange.

The legal and ethical exchange of information occurring at these NDIA forums has served to inform defense industry of government priorities, plans, challenges and needs, enabling better informed and more timely responses to DoD requests for information and proposals, while simultaneously offering industry the opportunity to inform DoD leaders about new and emerging technologies, capabilities and processes – and the need has never been greater.

Whether or not sequestration occurs, it is relatively certain that severe budgetary impacts will be thrust upon the DoD, creating treacherous ripple effects throughout the defense industrial base. It is especially in such times of uncertainty that non-profit organizations like NDIA can be of tremendous value in keeping the lines of communication open between the DoD and its industry partners via conferences and other similar information-sharing vehicles. Under current policy, this very capability and the professional dialogue it spawns is being severely constrained. Severely restrictive conference policies at DoD have gone so far as to single out non-federal entities like NDIA, all but eliminating the opportunity for transparent and ethical communication between industry and the government.

As you read the attached policy concerns of industry, please consider the value that honest and open communication between industry and DoD represents to the taxpayer and the warfighter alike.

Sincerely and respectfully,



Lawrence P. Farrell, Jr.
Lieutenant General, USAF (Retired)
President & CEO

1

ISSUE 1: Maintain a Responsive Defense Industrial Base During Budget and Infrastructure Reductions

As everyone from federal, state, and local governments is keenly aware, significant federal budget reductions will occur over the next several years to reduce the federal debt. It is no longer a question of if or when, but rather how much these reductions will be. For the last two years, Congress has been struggling to agree on a plan that will reduce the debt and not impact mandatory spending (Social Security, Medicare) and not raise taxes which has proven, thus far, to be unachievable. To resolve this impasse, Congress passed the Budget Control Act of 2011 which was intended to force an agreement on the necessary reductions, and in the event of failure, directed a mandatory, across-the-board reduction on all federal discretionary budget accounts. If Congress cannot reach an agreement by the statutory deadline, a sequestration must be applied to all federal budgets early in 2013. If applied, the mandatory sequestration cuts for defense would be $56.7 billion in fiscal year 2013, which is about half of the total cuts mandated for the entire federal government, and includes similar DoD cuts for the next nine years. These amounts would be in addition to the nearly $487 billion that are planned to be deducted from the DoD budget over the next ten years.

Whether the reductions are an across-the-board unplanned and potentially harmful sequestration action or a programmed rational process, the federal budget will be significantly lower. The pressure to reduce the defense budget will be much different than it has been in the past. This time, the overall health of the firms that supply the technologies our armed forces utilize will have a national security imperative. Qualitative superiority in weaponry and other key military technology has become an essential element of American military power in the modern era not only for winning wars but for deterring them. Sustaining that superiority will require world-class scientific and manufacturing capabilities that are currently resident in the defense industrial base. Irrespective of when and how much the defense budget reductions will be, DoD must have the ability to make reductions in a programmed and focused manner that will take into account the potential long-term or fatal impact on the defense industrial base. Continued first class support to our warfighters and equipment for providers of national security must be maintained.

Complete a Comprehensive Overview of Defense Manufacturing Issues

Although there have been many studies of industrial matters, none has produced a comprehensive overview of defense manufacturing issues. Much of the reporting has been anecdotal, and no study has compiled a list of manufacturing and process vulnerabilities such as single-source suppliers. A cooperative study between government and industry needs to be done. The recently conducted Sector by Sector, Tier by Tier (S2T2) assessment will develop a baseline of data across a wide swath of industry (including aircraft, shipbuilding, space, ground vehicles, missiles, missile defense, services, and information and communications technology). In the future the database and methodology will serve as a starting point for the DoD's wide variety of industrial assessments. This reservoir of knowledge will contribute to better acquisition decisions, help ensure realistic program objectives and reduce programming swings that disrupt industrial base investment. It will also contribute to DoD's merger, acquisition, and divestiture reviews and other industrial base policies.

Recommendation

Congress should consider directing the DoD to complete a study of the defense industrial base to insure that, at a minimum, there is effective management and delivery of processing and fabrication technology solutions, active support for a highly connected and collaborative defense manufacturing enterprise, a strong institutional focus on manufacturability and manufacturing process maturity, and active support for a healthy, sufficient and effective defense manufacturing infrastructure and a trained workforce.

Maintaining the Manufacturing Defense Industrial Base
U.S. national security depends heavily upon our domestic manufacturing capabilities and the 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. The segment that is not funded will eventually wither and industry will lose that capability, which will later take substantially more time and funding to be regained.

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 U.S. 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 such replacement is not always possible for certain defense-essential capabilities. Access to domestic sources may become a national security requirement. The current defense 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.

When absolutely necessary, the DoD will intervene to create and/or sustain competition, innovation, and essential industrial capabilities. If intervention is warranted, the DoD can use mechanisms authorized under Title III of the Defense Production Act (DPA)[1] 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. Title III of the DPA provides a set of broad economic authorities, found nowhere else in law, to incentivize the creation, expansion or preservation of domestic industrial manufacturing capabilities needed to meet national security requirements determined through extensive evaluation as both defense essential and in need of support.

Recommendation
As the defense budget continues to contract, Congress should carefully review the impact of these reductions as they pertain

Improving Manufacturing Research and Development
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 labs. Recent studies of best in class foreign R&D strategies have concluded that developing regional "clusters" of specialized R&D partners provides the most effective model for government, academic and industry innovation, and increases 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.

With respect to manufacturing R&D for national security, the DoD has a single program that is legislatively chartered to develop and transition manufacturing processes and fabrication required for the production and support of defense systems known as the DoD Manufacturing Technology (ManTech) Program (Section 2521 of Title 10 USC). For over 50 years, the ManTech Program has been DoD's investment mechanism for staying at the forefront of defense essential manufacturing capability. In accordance with DoDD 4200.15, investments in ManTech shall:

- Aid in the economical and timely acquisition and sustainment of weapon systems and components.
- Ensure that advanced manufacturing processes, techniques, and equipment are available for reducing DoD materiel acquisition, maintenance, and repair costs.
- Advance the maturity of manufacturing processes to bridge the gap from research and development advances to full-scale production.
- Promote capital investment and industrial innovation in new plants and equipment by reducing the cost and risk of advancing and applying new and improved manufacturing technology.
- Ensure that manufacturing technologies used to produce DoD materiel are consistent with safety and environmental considerations and energy conservation objectives.
- Provide for the dissemination of program results throughout the industrial base.
- Sustain and enhance the skills and capabilities of the manufacturing workforce and promote high levels of worker education and training.

[1] Public Law 81-774 1950

- Meet other national defense needs with investments directed toward areas of greatest need and potential benefit.

The effectiveness of this joint services program is well demonstrated in a report to Congress that identified over 100 projects funded by ManTech from FY03-FY05 which have been implemented and yielded a cost avoidance of $6.3 billion. The imminent concern is that the investment in the ManTech program, currently averaging $210 million in the President's FY11-FY16 budget, is not at the level required to cause substantial changes in the defense industrial base. A 2006 Defense Science Board study on the ManTech program concluded that the proper investment level for ManTech should be 1% of the DoD RDT&E budget, or about $700 million. This investment level would enable the DoD to pursue technical solutions for the most pressing defense manufacturing and industrial base problems facing the U.S. today and in the future. Even in the declining budget environment, funding should be preserved for programs which have demonstrated the ability to both enhance the department's capabilities and substantially reduce the cost of acquisition and support.

Recommendation
Congress and the Administration should support the formation and management of R&D clusters by offering a centralized process for creating and developing them and provide for collaboration amoung these clusters utilizing a 'hub and spoke" model. Collaboration amongst the clusters offers innovation and product development opportunities that drive technology transition into complex systems, thus resulting in the greatest benefits.

Further, NDIA recommends prioritizing an increase in funding for the ManTech program. In this time of budget austerity, we recognize that spending increases can be difficult; however, the substantial size of the cost avoidance should make investing in ManTech more approachable.

Improving Access to Raw Materials
Critical to the industrial base is the need for steady, long-term access to affordable raw materials. Sometimes having a domestic manufacturing capability is not enough, as in the case of secure access to raw materials. A US industrial base can depend too heavily upon materials which are not readily available or affordable, causing additional cost, schedule, or failure. The Government Accountability Office (GAO) concluded that the DoD lacks a consistent department-wide framework to monitor its supplier base. Policy should be developed on this topic with the input of industry.

Recommendation
Congress should consider establishing a federal-level working group to identify and act upon the multiple options available to DoD, such as stockpiling, pursuing trade violation cases, developing domestic/alternate sources of certain raw materials, and entering into long-term purchase commitments.

Funding for Ground Robotics Programs
The Joint Ground Robotics Enterprise (JGRE) under the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OSD AT&L) has been the champion of ground robotics for Joint Services. JGRE is the only robotics organization that is truly "joint," working with end users, commanders, planners, and vendors, creating unified roadmaps for ground robotics within the DoD and then funding its development. NDIA is concerned that JGRE's existence may be threatened due to budget reductions, which could lead to disjointed development efforts that would ultimately lead to more expensive stovepipe solutions.

The wars in Afghanistan and Iraq led to the rapid adoption of ground robotics by the US military for missions such as explosive ordnance disposal (EOD), combat engineering, and reconnaissance. These ground robots have saved many lives. Now, with a waning DoD budget and a reduced force, the next generation of ground robotic systems needs to be a force multiplier in order to preserve our national security.

Recommendation
NDIA recommends that the JGRE be preserved and fully funded so that it can execute on the ground robotics vision that it generated with joint services, allowing for an integrated manned/unmanned force that strengthens the US as the world's preeminent land power.
NDIA recommends further an increase in funding for research, development, testing, and engineering of ground robotics now and in the future.

Requiring Drive-by-Wire in Order to Ensure Robotics-Readiness
The foundation of any unmanned system is a navigate-by-wire capability, whereby electronics are used to control a wide range of vehicle operations. Today all commercial and military aircraft, for example, are fully fly-by-wire. In contrast, very few if any military ground vehicles are fully drive-by-wire. While often considered, this capability is typically eliminated for lack of funding reasons.

With the coming reductions in military funding it is no longer feasible to think in terms of unmanned ground vehicles as

specially designed platforms; rather the DoD needs to think in terms of enabling warfighters to operate the same ground vehicle in either a manned or unmanned mode depending on the mission and situation. While it is possible to retro-fit ground vehicles to be drive-by-wire, the cost is far greater than if the capability were to be integrated into the vehicle from the outset.

Making all military ground vehicles drive-by-wire would also serve to accelerate the development and utilization of autonomous capabilities. By providing a market of "robotics-ready" vehicles, a host of small, innovative companies would be incentivized and enabled to develop new sensor and software technology capable of being integrated onto these military platforms. Such innovation today is stifled by the economics of having to first retro-fit such vehicles in small volumes at an exorbitant cost.

Recommendation
The DoD should consider a mandate to require all new and re-fitted ground vehicles be made drive-by-wire. Such action would advance the adoption of unmanned systems tehnology.

Develop and Implement Appropriate FAA UAV Regulations
In February 2012, the Federal Administration Agency (FAA) Reauthorization Bill (Public Law 112-95) was enacted, giving the FAA 90 days to promulgate regulations that would ease access to US airspace by unmanned aircraft systems (UAS). The FAA was directed to expand the list of allowed operators, ease the conditions for UAS use, and integrate UASs into national airspace by 2015. There is increasing doubt that the FAA will be able to meet the initial goal of designating 6 test sites by December 2012, jeopardizing the planned January 2013 test site operational date. Further delay would weaken the US UAS industry, as foreign competitors proceed apace with their development efforts.

Recommendation
NDIA urges the FAA to expedite the test site selection and drafting of regulations as ordered by Congress for the sake of national security and potential use by law enforcement, including suitable safeguards for public privacy and safety.

2

ISSUE 2: Improve Efforts to Sustain Cybersecurity of Critical Infrastructure

Recognizing Cybersecurity as a National Security Threat Issue
A major concern within the government and industry is the connectivity to cyberspace and the use of cyber tools as a mission essential requirement for organizational viability and effectiveness, including warfighting, research, and commerce. Despite the functional imperative, most stakeholders remain ill-prepared to blunt or adequately defend against cyber attacks by determined and adaptive adversaries. Zero-day attacks, Trojan horses, logic bombs, bot nets, distributed denial of service attacks, phishing campaigns, and other nefarious attempts to disrupt cyber functionality are now within the daily lexicon.

Cyber attacks are the means of choice for *threat actors* (nation state, criminal elements, radical extremists, or non-affiliated hackers) whose aim is to steal technology and information, and degrade, disrupt, compromise or destroy the freedom of movement, operations, and security that the nation demands. As a preliminary matter, it is important to understand that the threat posed by cyber attacks is a threat to *national security* when it relates to the defense industrial base or other critical infrastructure.

The recognition by the DoD that cyberspace is an operational domain rightly places the threat to vital national interests, critical infrastructure, and livelihood in the proper perspective.[2] This designation sets the necessary conditions to meet challenges in cyberspace at a level comparable to other threats that our nation faces: air, land, sea, and space.

[2] *Department of Defense Strategy for Operating in Cyberspace* was published in July 2011 (available at www.defense.gov/news/d20110714cyber.pdf) and provides the strategic context and five separate initiatives to best posture the department to meet the pervasive challenges in the cyber domain.

There are multiple dimensions to consider when crafting any proposed solution or developing operating parameters. The key issue is to understand the magnitude of the threat. Just as planning and execution, doctrine, tactics, techniques and procedures, sustainment, training and workforce development are fundamental to military operations in traditional threat domains, so must these same characteristics apply to address cyber threats.

Recommendation
Congress and the Administration should establish a force structure, by building capacity and capability, while conducting mutual dialogues, agency-to-agency and agency-to-industry on prioritization of limited resources. A whole-of-government solution is required to achieve unified action toward a strategic end state. This solution requires the inclusion of industry partners who contribute innovation, resilience, and commitment to the cyber threats and who can be key to attaining the desired outcome of defeating threat actors. The momentum lost in recent controversies to pass legislation must be re-gained, and if anything, the legislative framework must address three basic questions:

- Who will be in charge of cybersecurity and provide leadership within the government?
- What are the basic definitions (e.g. critical infrastructure) and concerns of cybersecurity? and
- How will a whole-of-government approach be accomplished so that information sharing can begin earnestly? The nation cannot allow cyber threats to national security to continue.

Provide for an Educated Cyber Security Workforce
The need for a more robust educational initiative in the field of cyber security cannot be over-emphasized. In April 2010, the executive branch announced the National Initiative for Cybersecurity Education (NICE), an agency-wide education initiative that is being coordinated by the National Institute of Standards and Technology. NICE has four components:

1) National Cybersecurity Awareness;
2) Formal Cybersecurity Education;
3) Federal Cybersecurity Workforce Structure; and,
4) Cybersecurity Workforce Training and Professional Development.

Each component has one or more agency leads, but overall implementation of NICE is meant to be agency-wide.

The implementation of NICE will affect all of industry especially government contractors. For example, DoD is one of three lead agencies for component #4 above, Workforce Training and Professional Development.

NDIA strongly believes that the role of education in cybersecurity is at the forefront of any corresponding initiative. It is in the interest of government to partner with private industry and academia to ensure that NICE follows its current blueprint. The nation must streamline cyber professionals into the workforce. Credentials should be attained in a shorter time frame, with clear educational paths for cyber professionals that can be measured industry wide. Certification requirements, which assure both government and industries that a cyber professional's skills are current, should be a continuing part of this education initiative.

Recommendation
Congress should consider legislation, including amending the Workforce Investment Act[3], to direct the Departments of Labor and Education, as appropriate, to provide opportunities for workforce training and education in this unique area of national security, similar to and in partnership with the efforts currently underway to improve STEM education.

Foster Effective Partnerships between the Government and Private Industry
It is no longer enough to invoke the concept of "partnership" in a discussion of cybersecurity. Unfortunately, true partnership in cybersecurity does not yet exist between all of industry and government, and intra-industry.The conversation has turned into a series of platitudes that have produced few effective results. Some partnerships do exist between government and industry (e.g. the DIB Pilot program and the Department of Homeland Security's (DHS) work with Information Sharing and Analysis Centers (ISACs)), but overall the effort is a work in progress that must gain momentum. The concept needs to be further developed as an efficient working standard on how the government and industry will relate to each other, how industries will relate to each other, and how industries will be protected from liability when engaged in cybersecurity efforts. Industry must have a significant partnership role in the operational design of this concept because innovative technologies, rapid fielding, and development of operating principles stem from these vested partners. The DoD's recent interim rule which establishes a voluntary information program between the DoD and the defense industrial base, is a positive beginning.[4]

[4] U.S. Dept. of Defense, "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities" Federal Register, Vol. 77, No. 92 (May 11, 2012). Rules and Regulations. Page 27615 (available at http://www.ndia.org/Divisions/Divisions/Cyber/Pages/StudiesandReports.aspx).

Recommendation
The Administration should continue through its regulatory process to implement laws related to the improvement of cybersecurity in a way that encourages collaboration with private industry and focused on the defense industrial base.

Promote Trust and Security in the Implementation of the *Cloud First* Policy
In 2011 the Federal Government established a *Cloud First* procurement policy, which is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.[5] In addition to the fiscal savings on information technology systems spending, the additional capacity for users from this approach is fully justified.

Protecting the integrity of information is critical for user confidence, and absent this assurance, little progress with using a cloud effectively can be made. Successfully achieving this objective presupposes knowledge, trust, and reliability of any cloud service, whether private, public, or hybrid along with the attendant risks.

Potential solutions must fundamentally incorporate a composite trust component with multiple dynamic layers rooted both objectively and subjectively. Precise knowledge about the cloud construct, its associated data, and characteristics is essential to the user prior to making a decision (operational, business, or private) to enter a cloud environment. To meet this precise knowledge requirement, there are two considerations: (1) an *object identity* must be realized by the user after careful analysis of policies, technologies, and incentives, which combined provide an appropriate level of assurance; and (2) *subjective trust* must be established through observation of cloud activity to determine if the patterns of use and transmissions are consistent with expected types of cloud activity and whether the cloud architecture has the ability to recognize anomalous behavior.

Further, a challenge closely related to cloud computing is the process of managing voluminous data (e.g., health care records, financial transactions, human resources information, etc.) for swift retrieval and assessment. Technically called *big data* needs to be managed in a way which ensures efficient and secure access to this data while minimizing the possibility of threat actor access.

As DoD and federal users accumulate terabytes, petabytes and exabytes of information, each require adequate storage, effective transfer, and swift retrieval to support operational and business processes and management and protection requirements. Developing the means to conduct secure, effective and efficient processing of this information is a fundamental requirement that would eventually create actionable knowledge from huge data stores and avoid overwhelming analysts and decision makers with irrelevant information.

Recommendation
The Administration must carefully undertake the procurement of cloud and big data solutions. Verification of trust in a federated cloud environment is an essential precondition to meet the growing demands of data processing, management, and analysis at required network speed. Industry partner support and participation to develop processes and perfect necessary operating procedures is central to achieving this objective. A corresponding obligation is to design and maintain the requisite architecture to enable storage, retrieval, and analysis of voluminous, disparate, and unstructured data.

Manage and Deter the Insider Threat
Tied to the recognition that external threats determined to cause harm to businesses and our nation exist, is the realization of the internal threat. An organization's integrity to be breached by someone internal to the enterprise is particularly insidious. While potential loss of intellectual property, financial compromise, and outright theft of critical information can be anticipated and deterred from external actors, similar organizational perils that originate internally are more challenging to identify and defeat.

The way to combat insider threats in cybersecurity is to establish an organizational climate that values awareness, detection, and deterrence. Within DoD, there are explicit information assurance (IA) programs requiring mandatory compliance. Partners in industry follow similar practices and when instituted, cared for, and routinely inspected by senior leaders, are effective. While not all instances of insider threats can neither be predicted nor prevented, there are defensive practices that can be invaluable. For example, remaining alert to human factors and establishing contingency plans to manage insider threats as well as implementing deterrence initiatives can offer a defense-in-depth.

[5] Kundra, V., *Federal Cloud Computing Strategy*, 8 February 2011 (available at http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf)

Recommendation
Congress and the Administration should work to enhance and support existing efforts to eradicate insider threats from within government agencies.

Improve Situational Awareness through the People-Process-Technology Loop
Building improved situational awareness is founded on three fundamental areas that create a linked loop: people, processes, and technology. First, the human in the loop is essential – technology is a critical enabler to manage data and information flow, but comprehension (*i.e.* sense-making) is a human function. Second, repeatable yet adaptive processes are developed based on doctrine, techniques and procedures. These bases enable defenses and reactions in a comprehensive way and not merely ad hoc reaction. Finally, disparate technology must be carefully integrated both for facility of operations and for management to control effectively the flow of information. To that end, technology can enhance situational awareness of cyber threats through automated communication with early warning (information sharing) systems, rapid alerts to the end-user, and hyper-automated responses – essentially, in the course of minutes, technology can determine a threat instead of relying on human reaction, which may take days. The human user can then analyze the reaction and determine the threat sources. The loop continues, but, unfortunately, the loop described above (or any similar model) has not yet been widely implemented to gain efficiency.

Recommendation
The Administration should continue to determine and implement actions that would lead to improvements in situational awareness and effectiveness. Such actions should enable the advancement of each factor within the loop.

Continue to Carefully Consider Security Risks of Trends in Technology
Given the proliferation of technology and growing demand for wireless and mobile capability, protecting data and preventing intrusion are key objectives.[6] The growing trend of smart phones and tablet computers creates definite efficiencies in all workplaces. Increased technology capabilities raise concerns about the ability to conduct one's work anywhere with secure information exchange and access to classified and unclassified information on demand. Significant challenges include ensuring data security while it transits via networks, device security and integrity, and device software/hardware intrusion detection and response. These represent only a few of the challenges. Industry partners bring considerable technical capacity and possible solutions to resolve these issues. Commercial off-the-shelf technology provides affordable, available, and capable answers. Trusted data protection is necessary to meet requisite security needs. Again, the DoD-Industry partnership will blend policy and precise technical operating authority to match capability with requirements.

In addition, the growing use of social media has become a widely accepted business practice both in DoD and the private sector, but embracing the most popular tools comes with inherent risk. Social media can provide key indicators and warnings about potential threat actors, yet simultaneously present a probable conduit for phishing or spear phishing attacks or a temptation to circumvent established IA policies. As a practical matter, social media capability can benefit employee morale and establish a positive presence in the marketplace, but may also have the unintended consequence of increasing insider threat vulnerability. The challenge is to mitigate and manage incurred risk and potential vulnerabilities.

Three basic risks when using social media are: operational security, IT system compromise, and compromise of privacy data of employees. The growing cultural shift to share the most private information (both personal and organizational) with friends (and friends of friends) is at the heart of these risks.

Recommendation
Congress and the Administration should continue to consider carefully legislation and regulations which control and impact the use of mobile technology and social networks to ensure efficient work environments and freedom of speech coexist with the security of critical infrastructure.

[6] The *Symantec Internet Security Threat Report: 2011 Trends*, Volume 17 (April 2012) reveals the troubling statistical trends on smart phone data theft as the use of such devices becomes prevalent.

3

ISSUE 3: Address Energy Security Challenges

Invest in Energy Solutions

DoD is the nation's largest energy user. In recent years, DoD has launched several initiatives to reduce its fossil fuel use by improving energy efficiency (i.e. reducing wasted energy) and shifting to renewable energy sources such as biomass, hydropower, geothermal, wind, and solar technologies to meet operational and installation needs. Energy efficiency and renewable energy can benefit mission effectiveness, the environment, and the bottom line.

According to a recent report by the Information Technology and Innovation Foundation (ITIF),[7] which tracks energy innovation from basic science to research, development, and demonstration, DoD's energy innovation portfolio demonstrates that DoD invested $1.5 billion in FY2012 in energy innovation—$500 million more than in FY2009. Further, DoD supported early stage and applied research of clean energy technologies consistently between FY2009 and FY2012, while procurement of innovative energy breakthroughs nearly tripled between FY2010 and FY2011. DoD now invests nearly twice as much procuring new clean energy technologies than it does procuring commercial, off-the-shelf technologies. The Navy invested the most in energy innovation—committing nearly $500 million in FY2012 to next-generation technologies in electricity, transportation, and alternative fuels.

All military branches and defense agency offices are investing significantly in grid and power electronics innovations, as well as demonstration, testing, and evaluation of alternative fuels. Breakthroughs in these technologies suggest opportunities for commercial sector applications in the future.

Recommendation

Congress should continue to invest in the innovative energy solutions pursued by DoD. History has demonstrated that investments in challenges facing defense can have sweeping positive ramifications for civilian problems.

Maintaining DoD's Operational Energy Strategy

The DoD pursues operational energy strategy for the warfighters and defense installations through a small set of goals: ensuring the availability of resources, pursuing efficiency measures, and implementing conservation programs. Nevertheless, these key elements are insufficient, simply because the government cannot always guarantee access to reliable supplies of energy. These goals do not address how the mission will be accomplished without enough energy resources. To ensure mission sustainability when supplies are not assured, the DoD should incorporate an additional goal addressing energy reliance into its operational energy security strategy.

Defense installations and operations are highly dependent upon reliable delivery of large quantities of specific, high-quality energy resources. This dependency creates significant vulnerability, because of a highly uncertain outlook for resource availability, finite oil supplies and increasing demand by the developing world. DoD's response to energy shortages and increasing costs has been to pursue a variety of sustainability initiatives, including efficiency, conservation measures, and alternative resources.

Energy resilience metrics should be part of the overall performance metric, and should be considered in requirements development and acquisition processes. This shift in emphasis from assuring supplies to assuring mission preparedness will complement and reinforce the mandate that mission performance takes priority over energy consumption. This new focus will also ensure future planning addresses not just energy supplies, but actual mission performance for the widest range of circumstances.

Recommendation

Despite the challenge to transition to an energy strategy that incorporates resilience and adaptability to evolving conditions given planned budget constraints, shifting mission priorities, and a need for flexibility in a changing global energy reality, DoD should consider making resilience a focus for energy security. Such changes should be directly addressed in DoD's Operational Energy Strategy which provides a roadmap for incorporating energy considerations into current programs, processes, and institutions.

[7] ITIF, *Lean, Mean, and Clean II: Assessing DOD Investments in Clean Energy Innovation* by Megan Nicholson and Matthey Stepp, 1 October 2012

Utilizing Nuclear Power Technology

A stable, reliable base-load power generation that does not contribute to CO2 or methane emissions (such as coal-fired power plants or natural gas power plants) that is already available and suited well to both military facilities and smaller metropolitan areas is commonly referred to as a small modular reactor (SMR). Global demand for energy will only increase for the foreseeable future; the demand for electricity in the United States alone is projected to rise 30% by 2035. While wind and solar power are promising sources of plentiful energy and natural gas is seen as a reasonable replacement for coal-burning plants, only nuclear power provides the non-carbon base-load energy necessary for current and future needs. SMRs make sense as an affordable alternative to large-scale reactors and can serve as a source of continuous, reliable electric power generation. Military installations are the ideal place to test and implement SMRs, and the military has the ability to provide the long-term demand required to recoup SMR fabrication.

Recommendation

Congress should consider funding and cost sharing proposals to build prototype SMRs for use at military installations. This will allow adjacent civilian communities to benefit and ensure an uninterrupted and secure supply of energy while reducing DoD's energy costs.

Develop a Domestic Industrial Capacity to Supply Biofuel

Domestic crude oil production in the United States has increased over the past few years, reversing a decline that began in 1986. The United States is now a net exporter of refined petroleum products. According to the U.S. Energy Information Administration, over the next 10 years, continued development of unconventional oil resources combined with the ongoing development of domestic resources, may increase domestic oil production to a level not achieved since 1994.

The Secretaries of Energy, Agriculture, and the Navy have entered into a Memorandum of Understanding (MOU) to "assist the development and support of a sustainable commercial biofuels industry." The objective of the MOU is the construction or retrofitting of multiple domestic commercial or pre-commercial scale advanced drop-in biofuel plants and refineries. The MOU would support the Navy's goal of deploying a "Green Strike Group" by the end of 2012, and "Great Green Fleet" by 2016 fueled in part with a 50/50 blend of hydro treated renewable jet fuel (biofuel).

The Navy proposes to use authority under the Defense Production Act of 1950 (DPA) to develop a domestic industrial capacity to supply biofuel. In its FY2013 Congressional Budget Request, the Department of Energy (DOE) requested authority to transfer funds to the DPA Fund, offering the justification that it will support the MOU with the technical expertise to move pilot-scale demonstration projects to larger-scale production in support of the Navy's Green Fleet Goal. Agriculture, Energy, and the Navy expect to fund this initiative at $510 million in aggregate over three years.

Recommendation

NDIA recommends that Congress and the Administration continue to support the funding of the development of domestic industrial capacity to supply biofuel.

4

ISSUE 4: Evolve IT Acquisition in a Budget Constrained Environment

Evolve Information Environments

Information technology capabilities change quickly and despite having invested billions of dollars, the federal government still struggles to keep pace. Currently, the government faces numerous complex information challenges from dealing with legacy systems to adopting state-of-the-art mobile technology and from openness and transparency to protecting data and privacy.

Internet and web technologies have become the universal foundation for both business and mission operations. Technology has become so ubiquitous that on May 23, 2012, the President issued a directive entitled "Building a 21st Century Digital Government." This directive launches a comprehensive digital government strategy that is built upon four principles: information-centric, shared platforms, customer-centric, and security and privacy[8]. In 2010 the Office of Management and Budget (OMB) announced a 25-point implementation plan for restructuring federal information technology (IT). It required implementation within 18 months of five broad changes to agency IT: adopting light technologies and shared services; aligning the budget and acquisition process with the technology cycle; strengthening program management; streamlining governance and increasing accountability; and increasing engagement with the IT community. These initiatives, such as Cloud First and Shared First, are driven by the desire to reduce overall Government IT costs while increasing innovation and capabilities.[9]

The DoD Chief Information Officer (CIO) set a vision to develop an information environment that enables DoD and its partners to access securely information and services they need at the time and plece, and on approved devices of their choosing.[10] This future vision is based on merging mission operational needs with concepts previously embedded in separate net-centric strategies. The Joint Information Environment (JIE) is the DoD initiative to realize this vision. The JIE is to deliver increasingly optimized information, network, hardware, applications and governance for this environment across the Department. The initial focus areas that are to deliver capabilities are Data Center Consolidation, Network Normalization, Identity and Access Management (IdAM), Enterprise Services, and a single Security Architecture.

The OMB and DoD initiatives describe a fundamental change in how the Government acquires IT capabilities. These are necessary if we are to maintain information superiority while at the same time reducing the costs of acquiring, maintaining, and upgrading information sharing capabilities. To achieve these goals significant obstacles must be addressed. Current information environments are composed of many stovepiped, purpose-built legacy systems upon which Government depends and which architectures do not reflect the current emphasis on shared services. In addition, the adoption of a services-centric business model breaks the well understood acquisition paradigms as institutionalized in Department of Defense Instruction (DoDI) 5000 series. As stated in the Association for Enterprise Integration (AFEI, an affiliate of NDIA) study *Industry Recommendations for DoD Acquisition of Information Services and SOA Systems*, these approaches require changes to traditional roles, a re-balancing of the government-industry equilibrium, and a re-thinking of how integration and oversight are accomplished.[11] A services-centric environment demands greater dependency amongst its participants. This implementation has significant implications on issues such as performance, integration, culture, accountability and liability.

Recommendation

NDIA recommends the Administration revisits the implications contained in the AFEI study and increase its interaction with industry groups, such as the DI2E Industry Advisory Group. This should help pave the way for serious discussions on migration of legacy capabilities and measures necessary for fundamental changes to business models in ways that effectively support loosely-coupled, horizontally integrated services while still providing viable market incentives for industry.

[8] Digital Government: Building a 21st Century Platform to Better Serve the American People (Strategy), The White House, http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

[9] Federal Information Technology FY2013 Budget Priorities, "Doing More With Less", Steven VanRoekel, https://cio.gov/wp-content/uploads/2012/09/FY2013-IT1.pdf

[10] DoD Information Enterprise Architecture Version 2, DoD CIO, Http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2.0_Volume%20I_Description%20Document_Final_20120730.pdf

[11] Industry Recommendations for DoD Acquisition of Information Services and SOA Systems, July 7, 2008, SOA Acquisition Working Group, The Association for Enterprise Integration, http://www.afei.org

Improve Efficiency and Efficacy in IT Acquisition
Section 804 of the National Defense Authorization Act (NDAA) for Fiscal Year 2010[12] required the Secretary of Defense to develop and implement a new acquisition process for information technology systems based on the recommendations in Chapter 6 of the March 2009 report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology[13]. The NDAA language specified that the new IT acquisition process was to include early and continual involvement of the user; multiple, rapidly executed increments or releases of capability; early, successive prototyping to support an evolutionary approach; and a modular, open-systems approach.

AFEI convened an ad hoc, joint industry – government task force to address industry perspectives on the required new acquisition processes for information technology. The task force issued its report in June 2010, stating that industry believes the most difficult challenges lie with changing how government views IT acquisition and the processes used to define and buy essential capabilities.[14] The report recommended that DoD institute continuous development, test, and certification processes similar to those that drive commercial companies to deliver more trusted, standard, and off-the-shelf building blocks and endorsed the development of new software acquisition processes. NDIA is concerned that, to date, DoD has not complied with the requirements of Section 804.

The unintended consequences of well-intentioned legislation requiring Major Automated Information System (MAIS) reporting were created for large, hierarchical information systems projects developed under the waterfall model. These legislative requirements encumber and hinder development of the loosely coupled, web-based capabilities that our strategies envision. The consequences of these laws have been disincentives for innovative behavior and enlarged bureaucracy.

Recommendation
Congress should consider legislation that will automate oversight processes, define and mandate an enforceable enterprise-enabling role for government acquisition professionals, eliminate bureaucratic overhead, and mandate and reward specifically defined better speed-to-capability through a more general adoption of agile methods where appropriate. Moreover, the DoD should collaborate with industry groups, such as AFEI, to develop training and certification for programs managers, contracting officers and specialists, auditors, and technical representatives on how to contract for and manage agile software development.

5

ISSUE 5: Address Improvements Needed to the Procurement Process

Create an Industry/Government Partnership to Review Onerous FAR/DFAR Clauses
Concerning the access to commercial products, and acquisitions in general, onerous and likely unnecessary Federal Acquisition Regulation/Defense Federal Acquisition Regulation (FAR/DFAR) clauses continue to plague procurements and are a definite discouragement to commercial companies considering selling into the federal government. NDIA encourages simplified acquisition approaches, to include clarified and only necessary requirements. While there may be periodic reviews of FAR/DFAR clauses on a case-by-case basis, an all inclusive, focused review by stakeholders of all regulations would identify the most onerous requirements, as viewed by industry and the government. This type of review of standardization in requirements would potentially reduce costs to the contractor and enable those savings to be shared with the government. Lessons learned can be rolled into more far reaching standardization.

Recommendation
The Administration should conduct a full, all-inclusive review of FAR/DFAR clauses in an effort to standardize and streamline regulations while creating savings to the government.

[11] Industry Recommendations for DoD Acquisition of Information Services and SOA Systems, July 7, 2008, SOA Acquisition Working Group, The Association for Enterprise Integration, http://www.afei.org
[12] P.L. 111-84, National Defense Authorization Act for Fiscal Year 2010, SEC. 804. IMPLEMENTATION OF NEW ACQUISITION PROCESS FOR INFORMATION TECHNOLOGY SYSTEMS
[13] Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology, March 2009 http://www.acq.osd.mil/dsb/reports/ADA498375.pdf
[14] Industry Task Force Report, Industry Perspectives on the Future of DoD IT Acquisition - 2010 National Defense Appropriations Act, Section 804, June 6, 2010, The Association for Enterprise Information, www.afei.org

Protecting Critical Contract Services

Government service contractors continue to be an integral part of the defense industrial base and DoD can no longer execute expeditionary warfare without service contractor support. The defense services base continues to be a major source of defense innovation. NDIA promotes increased dialogue and a more collaborative partnership between government and services contractors.

Section 808 of the National Defense Authorization Act for Fiscal Year 201215 capped DoD spending for contract services in fiscal years 2012 and 2013 at the level of the President's request for fiscal year 2010. Among other requirements, the provision also required the Secretary of Defense to establish, for contracts and task orders awarded in FY2012 and FY2013 over $10 million, a negotiation objective for labor and overhead rates not to exceed those rates paid to the contractor in FY 2010. NDIA understands that Congress is considering additional legislation that would extend the temporary cap into FY2014. With budget uncertainty looming, the services industry continues to see decreases in services requirements and have accordingly reduced hiring and investments which will cause a future reduction in service industry technology innovation.

Recommendation

Congress should consider repeal or modification of the section 808 restrictions as currently implemented by DoD and oppose any further service contract restrictions. NDIA is aware of well intended legislative proposals that can collectively have a debilitating effect on hiring, investment, and resulting innovation that comes from the defense knowledge base industry. These restrictions discourge the innovative nature of the knowledge-based industry and contravene the current outcry for efficiencies in the government contracting process.

Address Counterfeit Electronic Part Problems

NDIA continues to monitor current and proposed legislation and regulations to establish new requirements and liabilities related to control of counterfeit electronic parts. It is expected that these policies will make contractors responsible for the detection and elimination of counterfeit parts throughout their supply chain. Contractors may be required to purchase from only "trusted suppliers" and establish new policies and procedures to reduce the risk of counterfeit parts migration into developed products. Contractors may also be required to advise the government when counterfeit parts are suspected or found. NDIA is hopeful that revised policy to address gaps in counterfeit parts policies within the supply chain will include the necessary dialogue between industry and government to avoid policy missteps during any implementation and that such dialogue may mitigate unintended consequences and unnecessary costs to the DoD and the taxpayer.

Section 818 of the National Defense Authorization Act (NDAA) for fiscal year 2012 required DoD to issue guidance on the detection and avoidance of counterfeit electronic parts in the DoD supply chain by September 2012. Congress is now considering a change to Section 818 that would allow the Department to reimburse the cost for rework or corrective action for counterfeit and suspected counterfeit electronic parts provided the contractor (1) has an operational detection and avoidance system as required under Section 818, (2) procured the parts from authorized or trusted suppliers or from the government as government furnished equipment, and (3) provided timely notice of the discovery to the government.

Recommendation

NDIA provided Congress with a detailed paper on counterfeit parts that addresses contractor risk-based mitigation policies, makes it more practical for DoD and industry to implement, incentivizes industry's detection and avoidance efforts, and addresses some of the root causes of counterfeits in the supply chain. NDIA advocates a better Congressional understanding of industry's supply chain challenges and ways that different industry sectors have undertaken to improve their quality assurance processes resulting in better detection and avoidance capabilities.

6

ISSUE 6: Ensure Efficiencies and Education in Department of Defense and Industry Processes

Establish a Disciplined Approach to Requirements
In a *Harvard Business Review* article titled "Delusions of Success"[16] the authors say "in planning major initiatives, executives routinely exaggerate the benefits and discount the costs, setting themselves up for failure." In the dedication to meet the challenges of austerity, DoD must focus on careful planning. Developing the requisite data and bid packages for acquisitions will require drawing upon the knowledge and experience of the existing industrial base. The past few years of experience have resulted in many acquisitions delays due to Congressional action or inaction, delayed DoD Budget execution through bridge contracts, and funding shortfalls from original planned awards and lower re-compete ceilings. Currently, the prospect of automatic budget reductions and declining defense requirements will further challenge the requirements process. These actions result in additional cost in time (and labor) incurred by the contractor. In addition, the increase in workload of preparing solicitations which can withstand the test of a post award protest and frequently required additional formal input to the government customer are impacting industry's "to bid or not to bid" decision process. These factors will ultimately have a negative impact on DoD's desire for more competition and "best value." NDIA can provide significant expertise and assist in establishing new norms for a revised approach to acquisition and be a trusted partner in sustaining industry capability while maintaining and assuring the competitive landscape.

NDIA believes that when developing acquisition plans, key issues should be addressed early in the process to determine the cost and value of competitive procurements:

- What is the time and expense to prepare the Request for Proposal (RFP), review by contracts and legal staff, etc.?
- What overhead expense will the government indirectly absorb from contractors who develop extensive proposals and in many cases demonstration assets?
- Has the cost and time for the evaluation of the proposals, the questions, reviews, orals, etc. been included in the budget and timeline?
- What is the likelihood and cost of a potential protest?
- Does the risk profile of the program allow sufficient time for an inexperienced company to perform at a surprisingly low bid price?
- What are the potential industrial base outcomes, e.g., will the competitors remain competitive after a major program is awarded?

Recommendation
To meet its requirements for leading-edge capabilities, DoD must provide industry better access to the requirements generation process and also develop programs which include an adequate mix of work and funding to sustain a capable workforce and physical infrastructure. A dialogue with industry on the impacts of increased overhead costs of proposal requirements, awards, and funding delays would be helpful to strengthen a disciplined acquisition process. Achieving these changes will require a revitalized effort by government and industry.

Outcome-Based Sustainment Strategies For all Major Weapon Systems
Section 2302 of Title 10, United States Code, requires the DoD to employ outcome-based sustainment strategies for all major weapon systems. Outcome-based strategies ensure operational readiness at the lowest operations and support cost, provide full sustainment cost visibility, and typically leverage the best capabilities of the public and private sectors through strong government/industry partnerships. The requirements of Section 2302 are based on the DoD's application of performance-based logistics (PBL) since the late 1990s, reinforced by two (1999, 2009) extensive product support assessment efforts and the recently completed PBL Proof Points Study. Both assessments as well as the Proof Points Study found qualitative and quantitative evidence of the superiority of the PBL business model for sustainment when implemented via long term, multiple-year business arrangements. This includes

commitments for readiness outcomes and transfer of risk to industry product support integrators (PSIs) via fixed-price contracts. The Proof Points Study found that 12 of 13 programs converted from transactional support to outcome-based support realized improved operational readiness at a reduced cost compared with their pre-PBL support.

Despite the statutory requirement for outcome-based strategies and the long successful history of PBL, over 80 percent of DoD product support is provided in a non-integrated, transaction-based manner. This transactional approach hides true costs, sub-optimizes inventory, degrades readiness and promotes stove-piped, non-integrated sustainment that minimizes public/private partnering.

Consistent with the PBL Proof Points Study, application of the PBL business model with its key enabling success tenets including use of 5-year contracts (plus 5 year option) for outcome-based sustainment, best use of government and industry capabilities via public-private partnerships, and incentivized, fixed-price contracts with industry assuring delivery of readiness outcomes will allow DoD to maintain support for the warfighter, especially in the lean budget years of the future.

Recommendation
The DoD should fully implement outcome-based sustainment including:

- Completion of Business Case Analyses (BCAs) for all currently fielded systems supported via a transaction based strategy;
- Full cost accounting in the development of BCAs to ensure meaningful cost comparisons;
- Common and consistent definition of depot core capability to enable effective public/private partnering;
- Competitive selection of end-to-end supply chain integrators for common items across DoD.

Full implementation of the PBL business model across all weapon systems will enable the DoD to reduce the estimated $270B per year expended on logistics and sustainment and redirect resources to critical priorities such as DoD modernization accounts.

Maintain the Highest Levels of Contractor Ethical Conduct
The defense industry is frequently exposed to the media focus on allegations of contractor misconduct. Notwithstanding these reports, the fact remains that there is insufficient data to support claims of widespread waste, fraud, or abuse in government contracting. The goal toward high levels of ethical conduct is supported by industry's focus on training in business practices and ethical conduct. Throughout the defense industrial base, company policies and practices increasingly foster transparency and accountability in working with government oversight agencies. These changes are grounded in a focus on self-governance. It has been two years since the Federal Acquisition Regulations required contractors receiving awards in excess of $5 million and with performance periods of 120 days or more to have a written code of ethics and business conduct. Mandatory disclosure rules require contractors to report when there is credible evidence of a violation in the law or significant overpayments. NDIA continues to support the highest levels of contractor ethics including effective policies, compliance training and internal controls to manage better compliance in all contracting requirements. As an industry association, NDIA has established guiding ethics rules for thousands of corporate members. Ethics policies and institutional compliance by industry result in high quality products and services, transacted in an ethical and transparent environment, at fair and supportable prices. (See NDIA's Ethics Code at the end of this publication).

NDIA encourages sustaining a broad-based effort between industry and the government to reinforce high ethical standards and responsibility in the entire acquisition process. NDIA stresses through its seminars and educational events, critically important procurement integrity information throughout the U.S. industrial base and recognizes that procurement integrity problems and ethical lapses negatively impact the public trust of government and industry alike. Adverse procurement integrity issues detract from public and private sector priorities to ensure that the federal procurement system is and remains fair, balanced, efficient and accountable.

NDIA is concerned that the government may be using suspension or debarment as punitive actions taken against contractors for alleged performance mistakes. FAR Part 9 provides that the Suspension and Debarment Official (SDO) has the authority to suspend or debar based on an allegation or charge in a criminal or civil matter, but such decision does not require a final judicial decision on the matter. NDIA is also aware of recently proposed legislation that SDOs must provide a final decision to suspend a company or person based on allegations of wrongdoing or charges of wrongdoing, prior to findings by a court of competent jurisdiction or convictions. This proposed legislation further mandates that a SDO official be established in each of the military departments and the Defense Logistics Agency (DLA) and further, changes the reporting requirements prohibiting the SDO from reporting to

the acquisition or IG function within DoD. NDIA would agree that the alignment of the SDO with the Inspector General's office does in fact create a conflict of interest. Nevertheless, there is no evidence that the organizational alignment of the SDO with the acquisition function presents that same conflict. In fact, there are sound examples where the SDO function is aligned with the acquisition function and works very well. The acquisition function better understands compliance challenges in government contracting

Suspension and debarment actions should be reserved as a remedy for egregious violations of the law or intentional fraud. Further, industry experiences suspension action with little or no due process. NDIA supports a process where suspension and debarment actions are proceeded by fundamental due process protections including adequate notice of the suspension and debarment concerns and 30 days to develop and submit a corrective action plan that will be evaluated prior to any implementation under suspension and debarment. The federal marketplace is critical to our national security and industry and government must work together to enforce existing laws, maintain effective checks and balances, and eliminate the potential for unethical conduct.

Recommendation
NDIA strongly opposes any legislation restricting the alignment of the suspension and debarment function with the acquisition function. NDIA further opposes the requirement for a final decision by the SDO on referrals of an individual or company for being charged with a federal criminal offense relating to the award or performance of a DoD contract.

Achieve DoD Process Reform (Better Buying Power) and Drive Toward Efficiency
An April 19, 2012, the Defense Business Board Report described the DoD acquisition process as a system that "continues to take longer, costs more, and delivers fewer quantities and capabilities." NDIA supports the Defense Business Board's efforts to link the DoD's organizations that "develop requirements, perform acquisition, and assign and manage budgets." Further, there is a need to balance the legitimate necessity for accountability in the public marketplace with our pressing necessity to increase process efficiency.

In 2010 DoD established the "Better Buying Power" efficiency initiative to increase efficiency and reduce costs as a critical objective, particularly in the current environment of budget austerity. Responding to DoD's request for suggestions in the design of the Better Buying Power initiative, NDIA joined other members of the defense industrial base to engage in real and meaningful efforts to increase process efficiency and thus reduce both government and industry costs. NDIA submitted nearly 200 separate recommendations focused on inefficient DoD processes and government unique practices that add cost with marginal value. In 2011, DoD issued the first draft of its Better Buying Power initiative.

On November 13, 2012, DoD issued the Better Buying Power 2.0 (BBP 2.0) as a refinement to the initial recommendations. BBP 2.0 encompasses 36 initiatives organized into seven focus areas. These include a new focus area that reflects the importance of the total acquisition workforce. The basic goal of BBP 2.0, as stated by DoD, is to deliver better value to the taxpayer and warfighter by improving the way the DoD does business. The seven functional areas include: (a complete copy of the DoD BBP 2.0 proposal can be found at NDIA.ORG/Government Policy)

1. Achieve Affordable Programs
2. Control Costs Throughout the Product Lifecycle
3. Incentivize Productivity & Innovation in Industry and Government
4. Eliminate Unproductive Processes and Bureaucracy
5. Promote Effective Competition
6. Improve Tradecraft in Acquisition of Services
7. Improve the Professionalism of the Total Acquisition Workforce

Recommendation
The Administration should consider directing agencies to conduct a cost benefit analysis prior to adding any new process restrictions and regulations to the procurement process. DoD would further benefit by performing a comparison of public and private sector cost of performance methodologies before imposing new compliance, audit, or oversight requirements.

Continue to Promote Education in Science, Technology, Engineering and Mathematics (STEM)
The economic growth and national security of every nation from product innovation to cybersecurity to the design and operation of sophisticated defense systems rely more than ever on a technically educated and skilled workforce. To maintain US economic and military advantages, the Nation must act swiftly and decisively to enlarge the STEM talent pool over the short and long term. Despite a historically high unemployment rate, there is an acute shortage of STEM professionals in select fields. In the short term, the skills gap may be alleviated by facilitating paths to permanent resident and citizenship status for STEM degree holders, especially those with advanced degrees. It is counterproductive to educate foreign nationals,

many of them at our expense, only to deny those who want to stay here the opportunity to do so. In the long term we must enhance STEM education nation-wide. Specific actions could include better training for teachers in STEM fields, incentives for STEM teachers, adoption of best practices for STEM education, and coordinated outreach to underserved student populations, including minority and female students. The status quo, with the US lagging behind its competitors in STEM education, is unacceptable.

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 has been vital to ensuring a superior fighting force. In both peace and war America's defense industrial base has allowed the U.S. 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 necessary to respond to any potential threat. This industrial base requires active management. The nation would be ill served by a crippled industrial base that lacked the requisite skills and capital standing to respond with alacrity to the demands that are placed upon it.

Ultimately, it is imperative we increase the number of students who are prepared and excited to enter vocational, undergraduate and graduate programs in STEM fields. Closing this gap is critical to sustain our national security supremacy and improve the technical competitiveness of America's workforce. Recognizing the national defense workforce is not just made up of scientists and engineers, NDIA has engaged with other partners such as the Manufacturing Institute to develop the Manufacturing Skills Certification System, announced by President Obama on June 8, 2011. This action is the first step in bringing sorely needed jobs back on-shore, and strengthening our manufacturing base to reduce the likelihood of another near term recession.

Recommendation
NDIA believes all stakeholders in national security should increase the development and support for unique, exciting, and inspiring ways to encourage young Americans to pursue STEM careers. With industry, government, and community involvement, NDIA believes this can be achieved and our national security workforce will be sustained and strengthened.

7

ISSUE 7: Reform Export Controls to Ensure Competitiveness of the US Industrial Base

Promote the Administration's Export Control Reform Initiative
Given the national security imperative of deficit reduction, it is critical that opportunities for US industry be competitive in the global marketplace are promoted. One way to continue helping US industry compete abroad is ongoing work to reform export control. This initiative remains essential to supporting the US defense and security industry's sustained leadership in innovation, new technology development, manufacturing capability and overall global competitiveness. While many of the overdue reforms can be accomplished administratively without new legislation, NDIA urges continued coordination and dialog among all agencies, defense industry, and Congress to ensure the proposed changes and reforms can be implemented to protect selected key US technologies while at the same time allowing US industry to be more competitive in the international defense and security market.

Further, NDIA supports the importance of armaments cooperation and coalition operations to attain our national security objectives, especially given the severe mandates of the Budget Control Act of 2011 to reduce federal spending, including defense spending. The success of coalition operations requires well trained and equipped coalition partners employing materiel and tactics that are fully interoperable and supportable in a timely manner during combined exercises and combat operations. Additionally, US forces should have the benefit of advanced technologies developed by friends and allies outside the US that offer near term opportunities as force multipliers. Both efforts allow sharing in the advantages offered by the timely

transfer of defense articles and technology among trusted partner and allied nations. Efficient sharing of defense technologies is critical to winning ongoing conflicts and ensuring readiness for tomorrow's challenges. Technology sharing is rightfully subject to export controls, but those controls must be administered in an efficient, predictable, and transparent manner.

Recommendation
NDIA strongly supports the Administration's efforts to reform the outdated US export control system. We recommend a structured, balanced approach that incorporates Congressional, regulatory, and industrial inputs as new export control approaches continue to be developed, removing needless barriers to international trade by creating a positive US Munitions List, moving many items that have no military national security concerns to the control of the Department of Commerce. In addition, it is imperative that technology transfers among US partners and allies be streamlined to operate at the speed of war.

Moreover, NDIA fully endorses the security cooperation reform initiatives by the DoD and specifically, its Defense Security Cooperation Agency (DSCA) efforts to transform its supporting Security Cooperation/Foreign Military Sales (FMS) business processes and to seek ways to accelerate the process from program conception to delivery to effectively build partner capacity/capability and strengthen defense relationships.

Implementation of the UK and Australian Defense Trade Cooperation Treaties
The US Defense Trade Cooperation Treaties with the UK and Australia, respectively, offer strong potential to enhance defense cooperation and exports with our two most trusted Allies. NDIA believes the treaties protect our national security and address fundamental problems in our current system of sharing technology with our close allies. NDIA understands these treaties require a separate set of licensing and record-keeping procedures. It is therefore important that implementation of these treaties be accomplished in a manner that enhances and does not degrade or further complicate the existing export Administration process.

Recommendation
The ongoing Export Control Reform Initiative should greatly simplify the implementation of these treaties. Failure to balance legitimate regulatory concerns and operational utility risks leaving companies with an unappetizing choice between the cumbersome, but well understood, International Traffic in Arms Regulations (ITAR) and a new vehicle perceived as promising but cumbersome and less understood than ITAR.

Trans-Atlantic Defense Industrial Cooperation
NDIA supports the continued emphasis devoted by NATO to the importance of Transatlantic Defense Industrial Cooperation (TADIC) as recommended by the NATO Industrial Advisory Group (NIAG) and endorsed by the Conference of National Armaments Directors (CNAD). The successful TADIC Conference in October 2011, co-sponsored by the CNAD and NIAG, reinforced the importance of the Administration's efforts to streamline export control procedures and the European Union's efforts to revise its export control directives to avoid unnecessary duplication. Further highlighted was the need to enable simpler and faster export licensing for inter-allied transfers, while meeting valid national security requirements through robust export control, industrial security, intelligence sharing and law enforcement measures.

Recommendation
As US, Canadian, and European defense budgets continue to be challenged by the mandate for budget control, NDIA believes that there should be increasing opportunities for enhanced transatlantic defense industrial cooperation and collaboration. The role of industry during these austere times will be critical for NATO to achieve its Smart Defense Initiative for multinational approaches to capability development.

Trans-Pacific Defense Industrial Cooperation
In its 2012 Defense Strategic Guidance for sustaining US global leadership in the 21st Century, the DoD states that

> *"the U.S. economic and security interests are inextricably linked to the developments in the arc extending from the Western Pacific and East Asia in the Indian Ocean region and South Asia, creating a mix of evolving challenges and opportunities. Accordingly, while the U.S. military will continue to contribute to security globally, we will of necessity rebalance toward the Asia-Pacific region."*

This document underscores the importance of our existing alliances as the foundation for our Asia-Pacific security, but also addresses the need for expanding cooperation with emerging partners to ensure a collective capability and achievement of common security objectives. The role of U.S. industry will be critical to help the DoD to achieve its strategic goals in areas such as, maritime domain awareness, C4ISR, integrated air and missile defense, cyber security, and integrated logistics, all of which will be constrained by export control procedures and the need for export licensing for inter-allied technology transfer.

Recommendation
The Administration should continue efforts to streamline

export control procedures and regulations with a focus toward building a Trans-Pacific Defense Industrial Cooperation similar to TADIC.

Increase Congressional Notification Threshold
The FY 2003 Foreign Relations Authorization Act modestly increased the thresholds for Congressional notification of Foreign Military Sales (FMS) and licensed transfers to NATO member states, Australia, Japan and New Zealand. In a March 2005 legislative request, the Administration recommended substantial increases to the arms sales and export notifications thresholds from $50M to $100M for defense articles or services; $14M to $50M for major defense equipment; and from $200M to $350M for defense design and construction services to these countries.

Recommendation
Enacting these increases will accelerate the process for FMS and licensed technology transfers by reducing the number of Congressional notifications of smaller sales and providing greater transparency in the Congressional notification process.

Extend Foreign Military Sales Program (FMS) Opportunities to Small Businesses
Small Businesses are being not included in the DoD's approach to using FMS as a means for countering budget cuts. Given that the FAR under provision 19.b exempts overseas actions from requiring competitive small business set-asides and the much lauded DoD goals for small business participation do not apply to FMS requirements, personnel assigned to support these requirements have no incentive to engage the small business community.

Increased FMS over the next two to three years is one way the US defense industrial base will survive the coming budget cutbacks. Given the aforementioned downward pressure on certain aspects of federal spending, especially the defense sector, small businesses supporting the defense industry and the DoD will necessarily seek new customers or disappear from the supply chain altogether.

In many instances the FMS "case" should be sent directly to a larger firm when a full vehicle or platform is being requested. An increased number of opportunities where small businesses are capable of meeting the contract requirements do exist. In addition, for requests from allied governments for sustainment support, repair and replacement parts, and additional services which do not require the OEM (and which many OEMs cannot perform cost effectively), small businesses are not considered.

Recommendation
Congress should consider legislation to direct DoD and the Small Business Administration (SBA) to ensure that small businesses have the opportunity to compete for FMS contracts and make efforts to support the industrial base to reach the fullest potential possible, enabling both large and small business to continue operations and meet our national security objectives.

8

ISSUE 8: Improve Small Business Awareness, Opportunity and Utilization in Government Contracts

Institute Parity among Small Business Socioeconomic Programs
The Section 1347[b] of the *Small Business Jobs Act of 2010* removed the "order of preference" from among the various socio-economic small business programs; however, NDIA believes that improvements are needed to allow contracting officers to decide freely when and where to create a set aside and for which category of small businesses.

The existing socioeconomic programs provide a diverse set of regulations on contract size limits, rules for competition, eligibility for set aside status, and so forth. Because of this, in practice, contracting officers do not always have the ability to "plug in" any one of the several categories of small businesses, including Women-owned, Service Disabled Veteran-owned,

HUBZone, etc. By simplifying the structure of these programs and making the structure universal, small businesses could have an even playing field in accessing government contract opportunities. Meanwhile contracting officers would have an increased flexibility seeking innovative solutions to serve the mission of the Department while creating a better opportunity of the governments meeting small business contracting goals.

Recommendation
NDIA recommends Congress consider legislation to create a universal set of standards for the entire community of small business socioeconomic programs.

Improve the Ability of Small Businesses to Research and Innovate
The Small Business Innovation Research (SBIR) program is designed to increase the participation of small, high technology, firms in federal R&D endeavors, provide additional opportunities for minority and disadvantaged individuals in the R&D process, and result in the expanded commercialization of the results of federally funded R&D. Current law requires that every federal department with an R&D budget of $100 million or more establish and operate an SBIR program. A set percentage of that agency's applicable extramural research and development budget—originally set at not less than 0.2% in FY1983, and currently not less than 2.7 in FY2013—is to be used to support mission-related work in small businesses.

The Small Business Technology Transfer program (STTR) provides funding for research proposals that are developed and executed cooperatively between a small firm and a scientist in a nonprofit research organization and fall under the mission requirements of the federal funding agency. Up to $150,000 in Phase I financing is available for approximately one year to fund the exploration of the scientific, technical, and commercial feasibility of an idea or technology. Phase II awards of up to $1 million may be made for two years. The STTR program is funded by a set-aside, initially set at not less than 0.05% in FY1994 and now at not less than 0.35%, of the extramural R&D budget of departments that spend over $1 billion per year on this effort.

Since Congress reauthorized the SBIR and STTR programs in the National Defense Authorization Act for fiscal year 2012, NDIA has been monitoring the subsequent implementation by the SBA of this much needed reauthorization and notes several concerns such as:

- Foreign Ownership: Proposed rules will allow foreign owned companies to compete for SBIR/STTR grants.
- Domestic Business Concerns: Instead of requiring "domestic" to mean U.S. owned, the SBA proposes only that a concern have a place of business located in the US. This could result in hundreds of millions of dollars of SBIR/STTR contracts.
- Venture Capital Ownership: It is difficult to determine if a venture capital company incorporated in the US is in actuality a foreign owned investor group
- Affiliation Rules: The new rules eliminate affiliation tests for large minority shareholders and exceptions are made for the SBIR program only, expanding the eligibility to firms that are not eligible for other SBA programs.
- Data Rights: Questions have been asked about the SBA's role in enforcing the legal rights of small business owners in terms of SBIR Data Rights

Recommendation
NDIA believes the SBA and related agencies should continually report on the impact of the rules on small businesses and the program overall particularly given the SBIR/STTR sections in the fiscal year 2012 NDAA legislation. In addition, DoD should design and enforce official policy for SBIR reporting goals and incentives as defined and consistent with the legislative intent outlined in the FY2012 NDAA legislation.

Set-Aside Programs for R&D
NDIA is concerned about existing FAR regulations which impede the ability of small businesses to compete in a set-aside program for government research and development (R&D) programs. FAR Part 19.502(b) reads: "In making R&D small business set-asides, there must also be a reasonable expectation of obtaining from small businesses the best scientific and technological sources consistent with the demands of the proposed acquisition for the best mix of cost, performances, and schedules." FAR Part 19 .502-2(b) establishes the general requirements for a total small business set-aside above the simplified acquisition threshold: (1) That offers will be obtained from at least two responsible small business concerns offering the products of different small business concerns; and (2) That the award from the set-aside will be made at fair market prices.

A rule was recently proposed to amend the Federal Acquisition Regulation (FAR) to clarify that contracting officers shall set aside acquisitions for research and development when there is also a reasonable expectation, as a result of market research, that there are small businesses capable of providing the best scientific and technological approaches. Because the proposed rule making is still in progress the final outcome is unknown; however, NDIA supports the position that R&D contracts

should be held to the same small business set aside standards as all other contracts. Currently, only 8% of R&D contracts are awarded to small businesses—far below the government-wide goal of 23%. Providing for set-asides with the same standard as other contracts could alleviate some of this shortfall.

Recommendation
Congress should act to ensure R&D contracts include small business participation at the same percentage goal as required of non-small business contracts.

National Defense Industry Association Statement of Defense Industry Ethics

Preamble
NDIA Member Companies should adhere to the highest ethical standards and seek to place the defense industry at the forefront of business ethics in America. At a minimum, NDIA members must adhere to applicable laws and regulations governing the conduct of their business. Moreover, entrusted to our care are the lives of Armed Forces Personnel who bear the ultimate risk for their Country to provide security to their fellow citizens. Thus, our common ethical mandate is a higher imperative than our individual business interests. This statement of ethics is intended to capture that mandate by setting forth common ethical principles and emphasizing particular practices that NDIA members may use to put those principles into action.

Mission
NDIA shall serve in a leadership role in setting high ethical standards for the industry and communicating industry efforts in this area to the public and government officials. NDIA will work with its membership to facilitate the practices set forth below.

Common Ethical Principles and Practices for NDIA Membership
NDIA members should aspire to the following ethical principles and make every effort to implement the following practices:

• Advance national security by promoting trust among the Defense Industry, our government customers, the U.S. public and our men and women in uniform.

• Strengthen the integrity of a federal procurement system that encourages competition, rewards technical innovation and ensures that American fighters have the decisive advantage on the battlefield and wherever else our nation's enemies may be found.

• Operate our businesses from a foundation of ethical readiness where economic pursuits do not overtake our responsibility to our soldiers, sailors, marines, and airmen, while acknowledging that America's technological and military preeminence are sustained by promoting the financial health of the defense sector.

• Contribute to the common good of our industry and promote industry ethics whenever and wherever possible by sharing best practices in ethics and business conduct among NDIA members and including ethics training in NDIA sponsored events.

• Implement effective ethics programs for company activities at home or abroad. When contemplating any international sale to a governmental or quasi-governmental buyer, it is imperative that effective measures be undertaken to ensure full compliance, not only with the letter, but also the spirit of the Foreign Corrupt Practices Act, as amended, and the FCPA's bar against improper payments to foreign officials.

• Establish effective mechanisms of control over employees and agents operating overseas to promote ethical conduct based upon principles, not geographic location.

• Protect U.S. national security when performing contracts with foreign parties by committing to compliance with U.S. export control licensing regimes, and with all anti-boycott and embargo requirements.

• Establish corporate integrity as a business asset, rather than a requirement to satisfy regulators, by making ethics integral to all aspects of corporate life and culture to create an environment where employees aspire to do the right thing.

• Recognize that self-governance is key to management's commitment to abide by ethical standards. Accordingly, charge Corporate Boards with responsibility for creating an environment where ethical conduct is the order of the day, including developing and implementing a corporate-level process or procedure to review company best practices, policies, and procedures governing ethics.

• Demonstrate the Company's and its leadership's commitment to ethics by making the Chief Executive the top ethics officer.

• Implement a formal company ethics program that includes a written code of conduct to communicate institutional values and expectations and guide employees and management in their decisions and conduct.

• Organize training programs as an integral component of company ethics programs to commit employees to the Company's written code of conduct, encourage them to discern the difference between right and wrong, and to act on that knowledge despite pressures to compromise standards.

• Establish and communicate procedures for employees to identify and report suspected violations of the code of ethics without fear of retribution, establish mechanisms to promptly and effectively communicate violations to the government, and promote full cooperation with government investigations.

• Ensure that employee reports of ethics violations receive immediate and objective attention from Company leadership by establishing a reporting system that promptly, within twenty-four (24) hours, informs the Chief Executive or his designee of any allegation that raises ethical implications.

• Establish written remedial measures for prompt and appropriate corrective action, including disciplinary measures, where instances of unethical conduct are discovered.

Vision

America's leading Defense Industry association promoting National Security

Mission

ADVOCATE: Cutting-edge technology and superior weapons, equipment, training, and support for the war-fighter and first responder
PROMOTE: A vigorous, responsive, government – industry national security team
PROVIDE: An ethical forum for exchange of information between industry and government on national security issues

Motto

Strength through industry and technology

Ms. Mary Ann Gilleece
Chair, Education and Lobbying Committee
NDIA Board of Directors

Mr. Glenn Baer
Chair, Government Policy and Advisory Division
NDIA

For additional information, please visit www.ndia.org or contact the Government Policy Department:

Mr. Peter M. Steffes
Vice President, Government Policy
Phone: 703-247-9470
Email: psteffes@ndia.org

Ms. Chandra Burnside
Senior Director, Government Policy
Phone: 703-247-2595
Email: cburnside@ndia.org

NDIA
National Defense Industrial Association

Vision

America's leading Defense Industry association promoting National Security

Mission

ADVOCATE: Cutting-edge technology and superior weapons, equipment, training, and support for the war-fighter and first responder

PROMOTE: A vigorous, responsive, government – industry national security team

PROVIDE: An ethical forum for exchange of information between industry and government on national security issues

Motto

Strength through industry and technology